UNIVERSIDAD CARLOS III DE MADRID

TRABAJO FIN DE GRADO

INTEROPERABILIDAD ENTRE SENSORES ÓPTICOS Y SEMICONDUCTORES PARA RECONOCIMIENTO POR HUELLA DACTILAR

GRADO EN INGENIERÍA ELECTRÓNICA INDUSTRIAL Y AUTOMÁTICA

Autor: Pablo Razquín Iracheta
Tutor: Raúl Sánchez Reíllo
Co-Tutor: Belén Fernández Saavedra

Leganés, 14 de julio de 2014

AGRADECIMIENTOS

RESUMEN

Hoy en día la tecnología se enfoca más y más a hacer la vida de las personas más cómoda. Es por ello que la biometría no ha tardado en sustituir a las maneras clásicas de identificación y de acceso como solían ser las contraseñas o las llaves.

Con su incremento en popularidad, son numerosas las compañías que diseñan sus propios dispositivos, distintos entre ellos no sólo por marca, también por tipo de tecnología o por manera de capturar la huella.

Debido a este hecho, el presente Trabajo de Fin de Grado (TFG) llevará a cabo un estudio de la interoperabilidad entre dos tipos de tecnologías, la óptica y la capacitiva. De este modo se podrá analizar el rendimiento que se obtiene al utilizar los dispositivos como se utilizaría en situaciones cotidianas. También se analizará la usabilidad de los distintos dispositivos para saber cuál es aquel que registra menos errores a la hora de utilizarlo.

Las muestras se obtuvieron en el Grupo Universitario de Tecnologías de Identificación (GUTI) a partir de usuarios que acudieron de manera voluntaria, creando así la base de datos (BBDD).

Con esta BBDD como punto de partida, se han obtenido los rendimientos en dos test analizando la tecnología usada, el primero siendo entre las tecnologías del mismo tipo y el segundo siendo una mezcla entre las tecnologías para saber qué tal interactúan. Además se ha creado una aplicación que permite analizar la usabilidad de los dispositivos utilizando los parámetros que se encuentran dentro de la base de datos.

El presente trabajo recopila todos los resultados obtenidos y las conclusiones alcanzadas a partir de ellos.

ABSTRACT

Nowadays technology is heading to give human beings a more comfortable style of life. This is why biometrics hasn´t taken much to start substituting the usual means of identification and access such as keys or passwords.

With its increasing popularity, many companies are now creating their own devices, with many differences between each Company. Not only because of brand, but also due to kind of technology used or the way the fingerprint is acquired.

Due to this fact, in this study has made an investigation on the interoperability between two kinds of technology, optic and capacitive. Doing so will allow to analyze the efficiency in a situation like the one it will be used on its daily use. It will also be analyzed the usability the different devices have to know which one achieves less errors when used.

Fingerprints were obtained in a research group at the university from users that volunteered, creating by this means the data base.

With this data base as a starting point, to analyze the interoperability, the devices were tested in two ways, depending on the technology used in them. The first of them being between the same technology and the second being a mixture between technologies to know how they interact. It has also been created an application that allows the analysis of the usability using the parameters that may be found in the data base.

The present document puts together all the results obtained and the conclusions obtained from them.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTADO DE ACRÓNIMOS

ADN	Ácido Desoxirribonucleico
BBDD	Base de Datos
CI	Concealed Interaction
CMC	Cumulative Match Characteristic
DET	Detection Error Trade-off
DI	Defective Interaction
DPI	Dots Per Inch
EER	Equal Error Rate
FAR	False Accept Rate
FI	False Interactions
FMR	False Match Rate
FNIR	False Negative Identification Rate
FNMR	False Non-Match Rate
FPIR	False Positive Identification Rate
FRR	False Reject Rate
FTA	Failure To Acquire
FTD	Failure to Detect
FTE	Failure To Enroll
FTP	Failure to Process
GFAR	Generalized False Accept Rate
GFRR	Generalized False Reject Rate
GUI	Graphical User Interface
GUIDE	GUI Development Environment
GUTI	Grupo Universitario de Tecnologías de la Identificación
IEC	International Electro technical Commission
ISO	International Organization for Standardization
JTC	Joint Technical Committee
LOPD	Ley Orgánica de Protección de Datos
RFID	Radio Frequency Identification
ROC	Receiver Operating Characteristic
SPS	Successful Processed Sample

1. Introducción

Este documento detalla el trabajo que se ha realizado durante el desarrollo del TFG. Se analizará la interoperabilidad y la usabilidad de sensores de huella dactilar con distinta tecnología. Estos sensores, gracias a la comodidad y seguridad que generan en los usuarios, ganan cada vez más presencia en la sociedad actual. Esta comodidad viene dada por el hecho de no tener que depender de elementos físicos ajenos al ser humano ni a recordar una contraseña, como pueden ser una tarjeta con banda magnética o una llave para una cerradura.

El proyecto se ha realizado dentro del GUTI, dedicado al estudio de los sistemas de identificación de personas. Este grupo pertenece a la Universidad Carlos III de Madrid.

Este primer capítulo tiene como objetivo proporcionar una visión general del trabajo llevado a cabo para su mejor entendimiento. En primer lugar se explicará el objetivo y la motivación, se continuará con el entorno socio-económico y se finalizará con la estructura del documento.

1.1. Objetivos y motivación

En la actualidad es necesario identificarse para realizar diversas acciones que se llevan a cabo en el día a día. El log-on en un PC, extraer dinero de la cuenta bancaria o acceder a lugares de acceso restringido son algunos ejemplos. Para evitar que se produzcan suplantaciones de identidad, los dispositivos biométricos son cada vez más utilizados. No sólo influye el factor seguridad, también afecta en gran medida la comodidad que aporta este tipo de identificación.

En contraposición a la seguridad y a la comodidad, se debe destacar el mayor grado de dificultad a la hora de instalar, utilizar y confiar en estos sistemas. Uno de los problemas más destacables en este ámbito es el hecho de que existen muchos tipos de dispositivos de captura de características biométricas, incluso dentro de una misma modalidad (huella, iris, firma, etc.). Estos dispositivos pueden variar en multitud de parámetros como pueden ser el fabricante, la tecnología utilizada o el tipo de muestra que captura. Es por ello que no siempre son capaces de interactuar de manera adecuada a la hora de realizar las identificaciones.

Debido a esto, el objetivo principal es estudiar la interoperabilidad entre dos de las tecnologías con las que están diseñados dos de los sensores, un sensor óptico y un sensor capacitivo. Para ello se harán dos test distintos. Uno en el que se compare el reclutamiento de un sensor con la verificación de ese mismo sensor. El segundo se combinará el reclutamiento de un sensor con la verificación del otro y viceversa. De este modo se obtendrán unas curvas con las que se podrá analizar cómo se comportan ambos sensores en los dos casos.

Además, un segundo objetivo es el análisis de usabilidad. Para ello se creará una aplicación que permita obtener gráficas con las que poder obtener la usabilidad de los

sensores y los errores que ocurren en cada uno de ellos según distintos parámetros que el usuario podrá elegir.

Para estos estudios se cuenta con una aplicación que calcula las tasas de rendimiento de los distintos dispositivos. Además, para determinar la usabilidad de los sistemas, se ha creado otra aplicación. Ésta, lee las BBDD que interesen al usuario y permite, mediante una GUI (Graphic User Interface) en MATLAB, obtener unas gráficas gracias a las cuales resulta sencillo determinar la usabilidad del sistema.

1.2. Entorno socio–económico y marco regulador

Se ha comentado con anterioridad que el reconocimiento biométrico aporta ciertos beneficios de comodidad y de seguridad a los usuarios que lo utilizan. Gracias a estas nuevas técnicas, se evitan tanto las suplantaciones como las pérdidas de los elementos que se utilizan hoy en día a modo de identificador.

Por ejemplo, al utilizar la biometría, se evita que una tarjeta de acceso a una zona restringida se pierda y acabe en manos de alguien que pueda hacer mal uso de ella. Otro ejemplo puede ser más útil para el día a día. A la hora de entrar al correo electrónico, las redes sociales, la cuenta del banco, y muchas más situaciones cotidianas, se necesitan contraseñas que pueden ser descubiertas sin demasiada dificultad por terceros y acceder de este modo a los contenidos privados que estas cuentas contienen.

Todo esto lo evita la biometría. Si a la hora de acceder a un área restringida todo lo que hay que hacer es posicionar el dedo en un sensor, no sólo es más cómodo, sino que además se está asegurando que sólo entra la persona que está autorizada para ello. El dedo, con su huella dactilar, es una característica única en cada ser humano, es por ello que dota al sistema de una seguridad muy elevada.

Para que estos sistemas sean realmente útiles, no sólo han de ser eficaces en cuanto a su software. También han de ser fáciles de usar para que la sociedad no los rechace y haya sido inútil todo el desarrollo. Es por ello que la usabilidad y la aceptación tienen tanta importancia y hay tal necesidad de realizar estos estudios. Si se consigue que un sistema biométrico sea intuitivo y fácil de usar, la sociedad será más propensa a utilizarlo y mejorará su calidad de vida.

Se ha mencionado también ciertos problemas que pueden acarrear estos sistemas. Uno de ellos es el coste que limita su expansión. Los sensores necesarios para su implantación son caros y por ello muchas veces la identificación biométrica queda restringida únicamente a situaciones muy específicas. Además, la sociedad aún no está acostumbrada a este tipo identificación. Debido al desconocimiento, existe cierto recelo a la hora de aportar las características fisiológicas de las personas por miedo a la propia suplantación de identidad y a la falta de privacidad.

Todas estas prácticas han de estar reguladas de alguna manera. Es por ello que se cuenta con normas y organismos que se encargan de dictar dichas normas. La ISO o el IEC son

dos ejemplos. Estas normas afectan a los dispositivos biométricos en su uso, para mejorar su rendimiento, y definen parámetros que permitan la interoperabilidad entre distintos sistemas.

La norma que afecta en mayor medida a este proyecto es la desarrollada por el comité de normalización ISO/IEC más concretamente por el grupo JTC1/SC37. Los estándares de este grupo se refieren a la biometría pero sólo los del conjunto 24713 tratan la interoperabilidad [1].

Por otro lado, no sólo son estas normas las que han de cumplirse. También se ha de cumplir la legislación española, cumplir con la Ley Orgánica de Protección de Datos (LOPD). Para respetar los derechos de los individuos que dieron sus muestras para este TFG, se ha seguido la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal [2].

1.3. Estructura del documento

Para poder aportar un hilo a todo el proyecto y que así se pueda ir siguiendo con facilidad se explicará a continuación la estructura que se ha seguido en este documento.

En primer lugar se da unas pinceladas acerca de conocimientos básicos sobre los que se cimienta el trabajo. Se explica la biometría y las distintas modalidades que podemos encontrar, profundizando más en la huella dactilar por ser el caso de estudio. Se introducen también las características bloques y procesos que sigue cualquier sistema biométrico además de los tipos de evaluaciones que se pueden realizar, centrándose en la usabilidad y la interoperabilidad, por ser, de nuevo, el caso de estudio.

Continúa con el cómo se diseñó el sistema de evaluación y qué pasos se siguieron a la hora de capturar las huellas para la BBDD que se ha analizado. Para estos análisis se ha creado una aplicación que será detallada, identificando los problemas que había a priori y cómo se fueron solucionando, las herramientas que se han utilizado y los factores que se han tomado en cuenta.

Por último se aportarán los resultados obtenidos de las pruebas que se han realizado con la aplicación y la BBDD y las líneas futuras con las que se podría continuar y ampliar este estudio.

2. ESTADO DEL ARTE

2.1. Definición de la biometría

Se entiende por biometría, la ciencia y la tecnología dedicada a medir y analizar datos biológicos [3]. Entrando en un ámbito más tecnológico se entiende de una manera un poco más concisa. Es una tecnología que permite la identificación de personas mediante el análisis de aquellas características que cada individuo tiene y que lo hacen único en comparación con los demás [4]. Estas características son muy difícilmente duplicadas, e imposible de perderlas u olvidarlas. Algunos ejemplos son la huella dactilar, el reconocimiento del patrón venoso del dedo o el reconocimiento facial. La biometría es un excelente sistema de identificación de la persona, se aplica en muchos procesos debido a dos razones fundamentales, la seguridad y la comodidad.

Entre las aplicaciones de identificación con biometría están el control de acceso biométrico, el control de presencia biométrico, el log on biométrico para aplicaciones de software a sistemas operativos, o cualquier otra aplicación de identificación que se realice mediante la incorporación de un lector biométrico.

2.2. Reconocimiento biométrico

Como se ha dicho antes, el reconocimiento biométrico se basa en los rasgos físicos de las personas, únicos para cada una de ellas. Dentro de estos rasgos se pueden dividir en dos grupos, los rasgos físicos (pasivos) y los rasgos de comportamiento (activos).

La medición de las características físicas de un individuo corresponde a la biometría estática mientras que las características de comportamiento corresponden a la biometría dinámica.

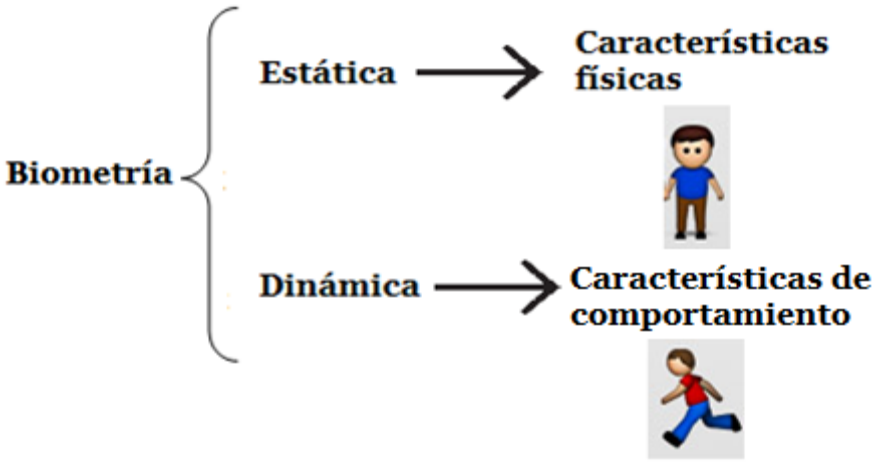


Figura 1 – Tipos de biometría

Las dos clases de biometría tienen grandes diferencias entre ellas.

Biometría estática

Se encarga de identificar a los usuarios mediante las características morfológicas, es decir, a los rasgos físicos.

Sistemas que realizan este tipo de identificación pueden ser los de huella dactilar o el iris.

Biometría dinámica

Identifica a los usuarios utilizando su comportamiento, no es algo propio del ser humano, cada uno tiene su manera de realizar una determinada tarea.

Sistemas que realizan este tipo de identificación podrían ser el reconocimiento de voz o la firma manuscrita.

2.2.1. Modalidades biométricas

Hay una gran variedad de modalidades biométricas para el reconocimiento de los individuos. Las más presentes hoy en día en la sociedad, en distintos ámbitos, son las siguientes.

2.2.1.1. Iris

El iris es la parte coloreada del ojo y tiene una textura muy compleja, como puede apreciarse en la figura 2. Esta textura es distinta en cada persona, incluso en gemelos idénticos. Es muy complicado que sean manipuladas quirúrgicamente y muy sencillo detectar intentos de falsificación, con lentillas por ejemplo.

Cuando se comenzó a utilizar esta modalidad, se requería una gran participación de los usuarios y unos equipamientos de gran coste. Ahora estos equipamientos son cada vez más económicos y más sencillos de utilizar.

Ventajas

No hay dos iris iguales y éstos no varían a lo largo de la vida de la persona. Por ello es muy útil para identificaciones y permite no tener que actualizar la información biométrica.

Desventajas

Los equipos siguen siendo caros y el grado de aceptación de usuarios es menor debido a sus métodos intrusivos.

Figura 2 – Iris humano [5]

2.2.1.2. Facial

El rostro es otro método comúnmente utilizado a la hora de identificar a un individuo. La cara tiene ciertas características que pueden ser aprovechadas y conjuntamente dar una exactitud elevada a la hora de distinguir entre una y otra.

La modalidad más utilizada por el momento es la que se basa en dos dimensiones (2D), con ella se mide la localización y la distancia entre distintos puntos de la cara como son los ojos, la barbilla o los labios. Figura 3.

La evolución de esta técnica está dando a lugar a la utilización de imágenes de tres dimensiones (3D). Esta nueva imagen se obtiene gracias al uso de múltiples sensores y a nuevos sistemas de procesamiento. Gracias a ello se pueden identificar más rasgos de carácter espacial obteniendo así textura y profundidad. Un ejemplo pueden ser los pómulos o los contornos de los ojos, no queda limitado a una imagen bidimensional. Figura 4.

Ventajas

Es un método no intrusivo por lo que tiene una mayor aceptación entre los usuarios. Además tiene una eficacia razonable. Tiene la ventaja de que la persona a identificar no tiene por qué ser partícipe en el reconocimiento. Es decir, sirve para el reconocimiento de sospechosos que hayan sido grabados.

Desventajas

En 2D afecta mucho la manera en la que se toma la imagen para el reconocimiento. Hay factores que pueden alterar el resultado como son el ángulo de la cara (inclinación, rotación o elevación), la iluminación en dicho momento.

Esto es algo que deja de ocurrir con la 3D. Aun así tiene los inconvenientes de que los sensores han de estar muy bien calibrados y sincronizados.

Es relativamente sencillo que el rostro de una persona se modifique mediante cirugía estética o un posible accidente por lo que no será tan sencillo reconocer a esa persona o incluso que el sistema haga una comparación errónea.

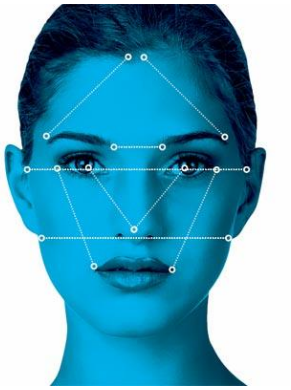


Figura 3 – Reconocimiento facial 2D [6]

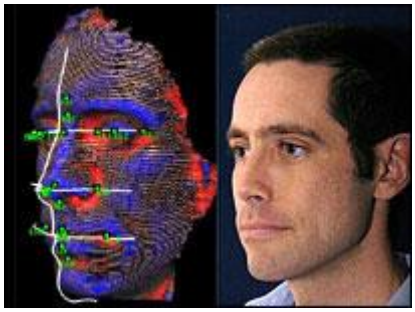


Figura 4 – Reconocimiento facial 3D [7]

2.2.1.3. Voz

La voz, aunque no lo parezca, es una combinación de varias características físicas de una persona. Viene dada por los labios, las fosas nasales o la forma y tamaño de la boca. Esto sin contar el tono que se alcanza con las cuerdas vocales de cada uno.

Para ello se obtiene una huella vocal que la determinan características como el timbre, el agudo, la edad o el género. No sólo eso, también es capaz de determinar el canal de transmisión para poder ajustarlo a otros canales. Además el sistema distingue si la voz es una grabación o una concatenación de palabras creadas con una herramienta.

Ventajas

Método poco invasivo con buena aceptación y sencillo en su utilización. Equipamiento de bajo coste y hace posible la autenticación de personas de manera no presencial.

Desventajas

El habla es un comportamiento que puede ser modificado con cierta facilidad, basta con estar resfriado o un cambio en la edad del usuario para que se vea variada. El factor ambiente también es muy importante ya que el ruido de fondo hará más complicado la autenticación de la voz.

2.2.1.4. Firma

Normalmente parece que la firma es una característica muy sencilla de imitar, pero no es así. No es sólo el trazo que se realiza con el bolígrafo lo que se analiza, se tienen en cuenta muchos más factores.

Al realizar la firma, de manera inconsciente, se aplica distinta presión en cada momento, se mueve el bolígrafo con mayor o menor velocidad, se realizan distintos giros, se inclina de manera distinta el bolígrafo o incluso se llega a detener la escritura en algunos puntos. Figura 5. Todos estos parámetros no son sencillamente imitables. Y al ser captados, crean un patrón único para cada individuo.

Ventajas

Es muy sencillo de utilizar y por ello goza de una gran aceptación.

Desventajas

La firma de las personas evoluciona con el tiempo de manera natural al repetir esa firma de repetidamente. No sólo varía de manera casual, también influyen las condiciones tanto físicas como emocionales de la persona a la hora de realizar la muestra. Un cambio de estas características podría dar lugar a una muestra que el sistema no sea capaz de procesar e identificarla con una ya existente.

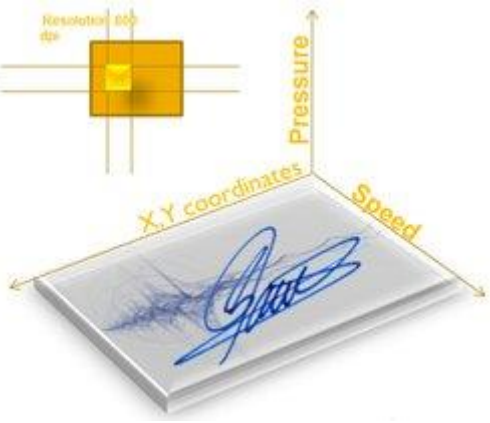


Figura 5 – Firma manuscrita [8]

2.2.1.5. ADN

El ADN es el elemento que contiene todas las características genéticas en los seres humanos. Lo podemos encontrar en el núcleo de todas las células que componen a una persona, más concretamente formando los cromosomas. Es único en cada una de las personas, a excepción de gemelos idénticos. Es por ello que resulta una característica biométrica imposible de imitar y muy distintiva de cada individuo.

Ventajas

El grado de identificación de personas es muy alto.

Desventajas

Los procesos requieren un coste muy alto que muchas veces justifica su no utilización. Debido a los complejos procesos que se han de realizar se ha de contar con un experto que esté pendiente de las muestras y el proceso. Además es un proceso altamente invasivo en el que el individuo ha de dar su material genético dando información acerca de su susceptibilidad a ciertas enfermedades, por ejemplo.

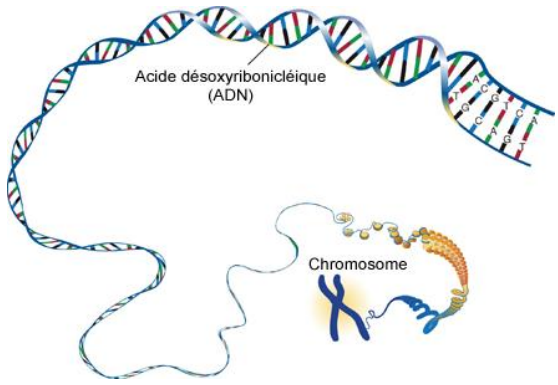


Figura 6 – ADN en los cromosomas [9]

2.2.1.6. Huella dactilar

La huella dactilar es la modalidad de reconocimiento biométrico más utilizada en la actualidad. Lleva varios siglos siendo utilizada, de manera más rudimentaria en sus inicios, y ha ido desarrollándose y mejorando gracias a las tecnologías existentes. Hoy en día se puede encontrar estos sistemas en gran cantidad de lugares como aeropuertos o en accesos a áreas restringidas, incluso en el desbloqueo de teléfonos móviles.

2.2.1.6.1. Características básicas de la huella dactilar y su extracción

Todos los sistemas dactiloscópicos se basan en tres principios:

1. Perennidad: Las huellas están presentes en las personas desde el sexto mes de gestación hasta la descomposición del cadáver.
2. Inmutabilidad: Las huellas no se ven afectadas en sus características por el desarrollo físico de los individuos.
3. Diversidad infinita: Las huellas dactilares son únicas e irrepetibles. Incluso los gemelos idénticos tienen huellas dactilares distintas.

Existe la posibilidad de almacenar las huellas dactilares como imágenes. Esto no es lo más adecuado. Tanto por seguridad como por la eficiencia del almacenaje.

Lo que normalmente se lleva a cabo es una copia de seguridad en algún lugar seguro con las imágenes de las huellas dactilares tal y como se toman del sensor. Es como si fueran fotos del dedo.

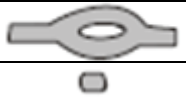
Sin embargo, en el lugar de implantación del sistema, no es recomendable tener estas imágenes. Lo que se tiene son unas plantillas de estas huellas. Es decir, se extraen las características que hacen únicas esas huellas presentes en las fotos y se crea un mapa con estos puntos básicos, las minucias. Éstas ocupan mucho menos espacio de almacenaje y son comparadas entre sí más rápidamente que una imagen.

Para comprender bien cómo se extraen estas plantillas, se ha de comprender la estructura y características de una huella dactilar, que se han comentado con anterioridad, y la interacción entre ellas para dar lugar a patrones únicos.

Una huella dactilar se compone, tanto por los relieves curvos o en espiral que normalmente se conocen, como de las intersecciones y bifurcaciones de estos relieves. Todas estas características se conocen como minucias. A continuación vemos los distintos tipos de minucias presentes en las huellas dactilares Tabla 1:

1. **Cresta independiente:** Cresta continua que no cruza con otra.
2. **Terminación:** Punto en el que la cresta termina.
3. **Bifurcación:** Punto donde una cresta se divide en dos distintas.
4. **Laguna:** Cresta que se divide y vuelve a unirse más adelante, creando una superficie cerrada.
5. **Isla:** Una cresta muy pequeña, prácticamente un punto.
6. **Espolón:** Similar a una bifurcación salvo que una de las ramas es muy corta.
7. **Cruce:** Dos crestas paralelas unidas mediante una tercera cresta.

Tabla 1 – Tipos de minucias

1	Cresta independiente	
2	Terminación	
3	Bifurcación	
4	Laguna	
5	Isla	

6	Espolón	
7	Cruce	

Todas estas minucias han de almacenarse siguiendo unos atributos. Los que se utilizan son los siguientes:

- Dirección: Determina la dirección de la cresta a la que pertenece.
- Posición: Posición geométrica de la minucia respecto a una referencia.
- Frecuencia espacial: Es la inversa de la distancia entre dos crestas consecutivas.
- Curvatura: Índice de variación en la dirección de las crestas.

El proceso de sacar un patrón se realiza siempre que se tome una muestra para compararla. Se obtiene la plantilla de minucias y esto será suficiente para realizar las comparaciones.

Hay algunas razones por las que se realiza este proceso de minucias:

- Cada huella dactilar tiene entre 30 y 40 minucias.
- No se puede reconstruir la imagen de la huella dactilar a partir de una plantilla de minucias. Aumenta la seguridad.
- La plantilla se puede comprimir con cualquier algoritmo de compresión de datos.

Ventajas

La huella dactilar es una técnica que ya ha sido ampliamente probada en distintas aplicaciones. Los costes de implantación son bajos y la aceptación de la que goza es buena en parte debido a ser poco invasivo.

No se puede reconstruir la imagen de la huella dactilar a partir de una plantilla de minucias. Aumenta la seguridad.

La plantilla se puede comprimir con cualquier algoritmo de compresión de datos.

Desventajas

Las huellas dactilares no son una característica biométrica difícil de imitar. Además puede suceder que las personas de avanzada edad o las que realizan trabajos manuales tengan una huella más degradada que la persona media. Dificultando su reconocimiento.

2.3. Sistemas biométricos

Un sistema biométrico realiza un proceso, mediante análisis y comparaciones, que permite identificar a una persona por unas características propias de cada ser humano. Ahora se detallará el funcionamiento de un sistema biométrico y los pasos que se llevan a cabo.

2.3.1. Bloques

Estos procesos los realiza el sistema biométrico. Hay muchos tipos de sistemas pero todos ellos comparten una estructura común. Figura 7.

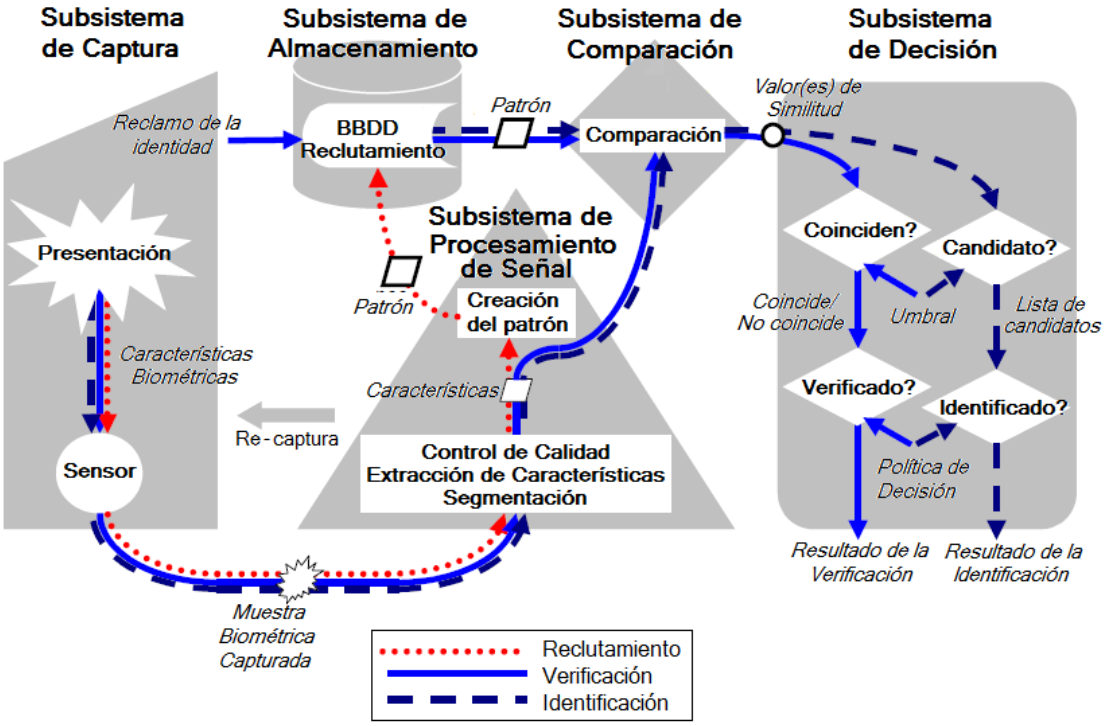


Figura 7 – Componentes de un sistema biométrico genérico [10]

Se puede dividir el sistema global en varios bloques como puede verse en la figura 7. Estos serán los subsistemas de captura, procesamiento de señal, almacenamiento, comparación, decisión, transmisión y administración.

Subsistema de captura: Es el encargado de capturar la muestra del rasgo biométrico y digitalizarlo para poder analizarlo posteriormente.

Subsistema de procesamiento de la señal: Mediante un algoritmo obtiene de la muestra un vector de características. Consta de varias etapas:

- Segmentación: Localiza en la imagen la información útil para el proceso.

- Extracción de características: Se obtienen las características esenciales para identificar a la persona.

- Control de calidad: Se asegura de que todas las anteriores etapas se han realizado de manera correcta.

Subsistema de almacenamiento: Almacena el patrón de cada muestra perteneciente a cada usuario durante el reclutamiento. Este almacenamiento puede realizarse en varios lugares, por ejemplo en una BBDD o en un token.

Subsistema de comparación: Al recoger una muestra nueva este subsistema compara la nueva con el patrón almacenado previamente. Varía según el proceso en el que se encuentre el sistema, se detallará más adelante las etapas que componen el proceso, en el apartado 2.3.2.

Subsistema de decisión: Recibe los datos del subsistema de comparación y se compara el valor obtenido con el umbral del sistema. A partir de esta comparación, se decide cómo proceder.

Subsistema de transmisión: Se encarga de llevar los patrones, el vector de características o la muestra capturada de un subsistema a otro.

Subsistema de administración: Gestiona las políticas y el resto de subsistemas.

2.3.2. Proceso de un sistema biométrico

El funcionamiento del sistema biométrico se divide en dos etapas:

1. Reclutamiento:

   Es la primera fase en la que el usuario se presenta ante el sistema biométrico. En ella que se adquiere la primera muestra de la característica biométrica que se va a analizar y se obtiene el patrón.

   Esta etapa tiene como finalidad tener en la BBDD un patrón identificativo único para un cada usuario. Este patrón será el utilizado para realizar las etapas posteriores del reconocimiento, la verificación y la identificación. Es por ello que se trata de la fase más importante de todo el proceso.

   Para realizar el reclutamiento de manera segura y que las muestras sean de buena calidad y aptas, ha de haber un operario que supervise la toma de muestras.

2. Reconocimiento:

   Se divide en dos procesos.

Verificación: Es el reconocimiento del usuario que declara su identidad. Se busca el patrón de ese usuario que se tomó en el reclutamiento y se hace una comparación 1:1. El resultado que se nos ofrece es un valor de similitud. La aceptación o el rechazo dependen ya del umbral que tenga el sistema y del valor de similitud.

Identificación: En esta fase el usuario no se identifica, se trata de reconocer a la persona de entre todos los usuarios de la BBDD. Se realiza una comparación 1:N. El sistema devuelve una lista de candidatos.

Identificación correcta: Si el usuario se encuentra dentro de esta lista.

Identificación incorrecta: Si un usuario registrado no se devuelve en la lista o, si para un usuario no registrado, se devuelve una lista.

Se cuenta con dos tipos de identificación. En la open-set es posible que usuarios que no han sido reclutados utilicen el sistema. En el closed-set todos los usuarios que utilizan el sistema han sido reclutados.

2.4. EVALUACIÓN DE SISTEMAS BIOMÉTRICOS

Las evaluaciones se realizan con el fin de saber si un determinado sistema cumple o no determinados requisitos. Este proceso ayuda a dos partes distintas, a los fabricantes y a los consumidores. Dan a conocer las ventajas, los inconvenientes y las mejores aplicaciones para cada tipo de tecnología. Su inconveniente principal es el coste que conlleva.

2.4.1. Tipos de evaluaciones

Contamos con varios tipos de evaluaciones:

1. Evaluación de rendimiento

   Es la más común de todas las evaluaciones y se ocupa de medir el rendimiento técnico, es decir, la precisión y la velocidad del sistema.

   Aporta la información más relevante como son las tasas de error del sistema y los tiempos de procesamiento. Las tasas de error miden la precisión de un sistema biométrico. Más concretamente miden el porcentaje de usuarios en los que ha habido un fallo de reclutamiento y el porcentaje de usuarios que han sido falsamente aceptados o rechazados en la verificación/identificación. Los tiempos de procesamiento representan el tiempo que tarda el sistema en realizar todos los procesos que necesita. A menor tiempo de procesado, mejor.

También tiene otras clases de análisis. Se encargan también de ver qué factores pueden afectar a su rendimiento, es decir, cómo funcionan las medidas del rendimiento frente a la variación de los factores que pueden llegar a influir al sistema una vez en uso.

- Entorno: Cómo afectan, y en qué medida, factores como temperatura, iluminación o ruido.

- Usabilidad: Estudia el rendimiento con distintos tipos de familiaridad con dispositivos de este tipo y distintos niveles de destreza.

- Interoperabilidad: Evalúa el rendimiento cuando las muestras o los patrones son generados por otros sistemas biométricos.

- Escalabilidad: Mide la capacidad del sistema a adaptarse a una BBDD en constante aumento.

- Fiabilidad: Analiza la frecuencia de los fallos y la capacidad del sistema seguir funcionando cuando ya han ocurrido.

- Robustez: Observa la habilidad del sistema a trabajar con datos que presentan ruido.

- Disponibilidad: Estudia el porcentaje de tiempo en el que el sistema está listo para usarse.

- Tiempo de respuesta: Analiza el tiempo que un usuario está a la espera de que el sistema tome la decisión.

- Sostenibilidad: Se obtiene el esfuerzo para mantener el sistema a corto y largo plazo.

2. Evaluación de conformidad

   Observa si la implementación del sistema cumple con requisitos específicos.

3. Evaluación de seguridad

   Es un tipo de evaluación de conformidad en la que se analiza los requisitos de seguridad. Normalmente requiere conocer las tasas de error del sistema por lo que es imprescindible incluir una evaluación del rendimiento.

   También se evalúan las vulnerabilidades del sistema.

4. Evaluación de aceptación del usuario

   Estudia el grado de aceptación del sistema por parte de los usuarios. Esto se realiza preguntando la opinión de los usuarios que han utilizado el sistema.

5. Evaluación de privacidad

   Analiza si el sistema cumple con la regulación de protección de datos del usuario.

6. Evaluación de coste/beneficio

   Evalúa si son rentables los procedimientos.

Se detallarán más a fondo las evaluaciones de rendimiento, interoperabilidad y usabilidad por ser el caso de estudio de este TFG.

2.4.2. Rendimiento

Se cuenta con tres tipos dependiendo de las condiciones en las que se desarrolle la evaluación. Se cuenta con la tecnológica, la de escenario y la operacional.

La tecnológica analiza el rendimiento de los algoritmos utilizando una BBDD genérica. El usuario no presenta la muestra en tiempo real, se utiliza una BBDD, por ello se denomina una evaluación offline. Podrá repetirse la evaluación una y otra vez siempre que se utilice la misma BBDD.

Tiene la ventaja de que, al utilizar una BBDD ya existente, no se tiene en cuenta la interacción que efectúa el usuario con el sensor. Por ello permite realizar un gran número de comparaciones y es útil usarlo en las primeras fases de desarrollo ya que sirve para perfeccionar el algoritmo que se usará más adelante.

En cuanto a la de escenario, calcula el rendimiento cuando el sistema está influido por unas condiciones controladas. De este modo se asimila en gran medida a lo que ocurre en la realidad cuando varios factores pueden llegar a influir en la toma de muestras. Las muestras se recogen en tiempo real. Como se ha visto antes, dependiendo del almacenamiento será online o una mezcla entre online y offline. En la online los usuarios darán su huella y se obtendrá la decisión del sistema en tiempo real. La mezcla es en la que se obtiene la muestra en tiempo real pero se realizan las comparaciones posteriormente.

Aquí se evalúa el sistema biométrico incluyendo la adquisición de la muestra pudiendo así comprobar los efectos del entorno y de la interacción entre el usuario y el sensor. Este tipo de evaluaciones se utiliza más a menudo cuando ya se conoce la aplicación que se va a utilizar y se desea comprobar que ocurrirá con algún factor en concreto antes de su implantación. También es muy útil para decidir de entre varias soluciones cual se adecúa más a cada aplicación que se le vaya a dar.

Por último tenemos el operacional. Esta es la evaluación más completa. Consiste en analizar el rendimiento de un sistema en su totalidad en el entorno real. Podemos llamarlo también prueba piloto pues simula exactamente la aplicación final. Dado este

fin, las muestras se toman online y ninguno de los factores está controlado. Esta evaluación permite saber si el sistema necesita ajustes, el rendimiento y si este rendimiento se ve afectado por alguno de los factores que se puede encontrar en una prueba real.

Algunos problemas que presenta pueden ser por ejemplo el evaluar a los usuarios, es decir, saber si el usuario que lo utiliza es genuino o impostor. Una solución alternativa es monitorizar la actividad. Se suele llevar a cabo en grandes proyectos que requieren una larga implantación.

Dentro de los análisis de rendimiento se cuenta también con las tasas de throughput. Se encargan de definir entre qué instantes se va a contabilizar el tiempo. Debe proporcionarse información del tipo de sistema que se está utilizando para medir esos tiempos. Se usan medidas estadísticas básicas como la media aritmética, mínimos, máximos y desviación típica.

2.4.3. Tasas de error

Las tasas de error son las que miden la precisión del sistema a la hora de identificar a una persona. Con ellas se obtiene una proporción del número de errores y dependen del número de comparaciones realizadas y de los umbrales.

Teniendo en cuenta las distintas etapas de un sistema biométrico, se pueden identificar distintas tasas de error para cada una de ellas.

Proceso de adquisición y procesado de señal:

i. Failure to Enroll (FTE): Proporción de usuarios que no han podido terminar el reclutamiento.

   Dentro de este apartado se encuentran aquellos que no han podido presentar la muestra biométrica, de los que no se ha obtenido una muestra de calidad suficiente y los que aun habiéndolo hecho correctamente ha sido imposible verificarlos.

   Lo adecuado es que se defina un procedimiento de cómo efectuar el reclutamiento.

ii. Failure to Acquire (FTA): Proporción de intentos de verificación o identificación para lo que el sistema ha fallado en la captura de una muestra con suficiente calidad.

   Dentro de esta tasa se incluye los intentos en los que la muestra no puede ser presentada o capturada, en los que el proceso de segmentación o extracción de características fallan y en los que no se obtienen una muestra de suficiente calidad.

Esta tasa depende en gran medida de los umbrales establecidos para la calidad de las muestras, el número de veces que se le permite al usuario presentar la muestra y el tiempo máximo del que dispone este usuario para llevar a cabo este proceso.

Proceso de comparación y decisión:

i. False Non-Match Rate (FNMR): Proporción de muestras biométricas, adquiridas de usuarios genuinos, que han sido falsamente declaradas que no coinciden con el patrón. El propio nombre de esta tasa indica que sí debería haber una coincidencia ya que es el mismo usuario (El valor de similitud no alcanza el umbral establecido).

ii. False Match Rate (FMR): Proporción de muestras, adquiridas de usuarios impostores en intentos de zero-effort, que han sido falsamente aceptadas. (El valor de similitud alcanza, o supera, el umbral establecido).

   En este caso no se deben tener en cuenta las muestras pertenecientes al mismo usuario, teniendo en cuanta que no es la muestra correcta, ya que hay cierta relación entre ellas.

Proceso completo:

1. Verificación:

   i. False Reject Rate (FRR): Proporción de transacciones que han sido incorrectamente denegadas.

      Dentro de esta tasa se tienen en cuenta las transacciones denegadas debido a un fallo en la adquisición o a no alcanzar los umbrales de comparación. Por ello se debe documentar el número de intentos permitidos, los umbrales de calidad y los umbrales de decisión.

   ii. False Accept Rate (FAR): Proporción de transacciones de impostor de tipo zero-effort que han sido incorrectamente aceptadas.

      Al igual que en el FRR, una transacción depende de los intentos según lo que se haya decidido para el sistema en cuestión. También deberá documentarse este número de intentos con los umbrales de calidad y decisión.

   iii. Generalized False Reject Rate (GFRR): Mide el rendimiento del sistema en relación con el rechazo de usuarios genuinos de manera conjunta incluyendo los procesos de reclutamiento, la adquisición de la muestra y la comparación.

   iv. Generalized False Accept Rate (GFAR): Mide el rendimiento del sistema en relación con la aceptación de usuarios impostores de manera conjunta

incluyendo los procesos de reclutamiento, la adquisición de la muestra y la comparación.

2. Identificación:

   i. False Negative Identification Rate (FNIR): Proporción de transacciones de identificación para usuarios que se encuentran reclutados dentro del sistema, para los cuales el identificador correcto del usuario no es incluido en la lista de candidatos devuelta por el sistema.

   ii. False Positive Identification Rate (FPIR): Proporción de transacciones de identificación para usuarios que no se encuentran reclutados dentro del sistema, para los cuáles el sistema devuelve una lista de candidatos que contiene algún usuario.

   iii. Identification Rate: Proporción de transacciones de identificación llevadas a cabo por usuarios que se encuentran reclutados dentro del sistema para las cuáles el verdadero identificador de usuario es incluido dentro de la lista de candidatos.

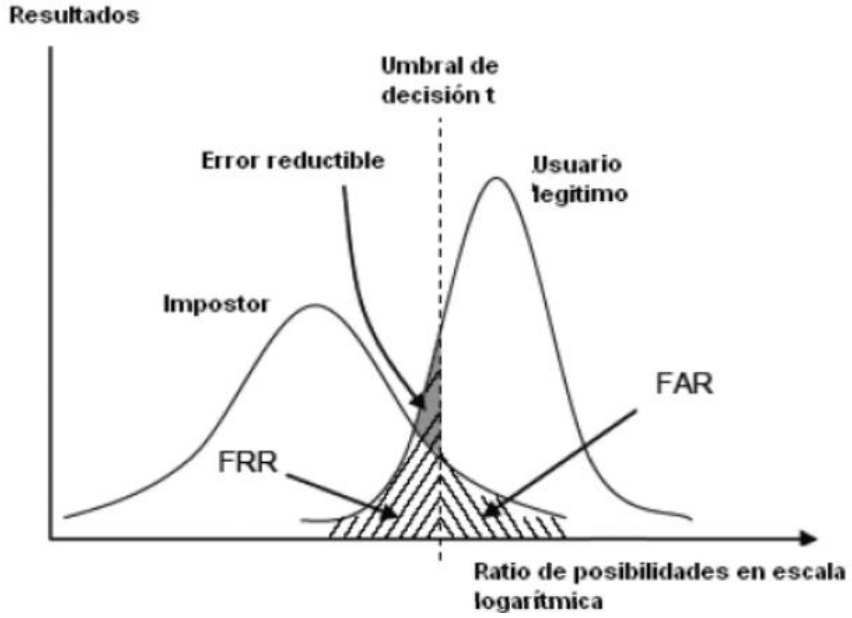


Figura 8 – Umbral [11]

Existen también curvas de rendimiento:

Receiver Operating Characteristic (ROC):

Dan información de cómo varían las tasas de falsa aceptación, tanto FMR como FAR, frente a las tasas de falso rechazo, FNMR y FRR.

En el eje de abscisas se representa la FMR/FAR. En el de ordenadas, 1-FNMR/1-FRR.

Puede verse un ejemplo en la figura 9.

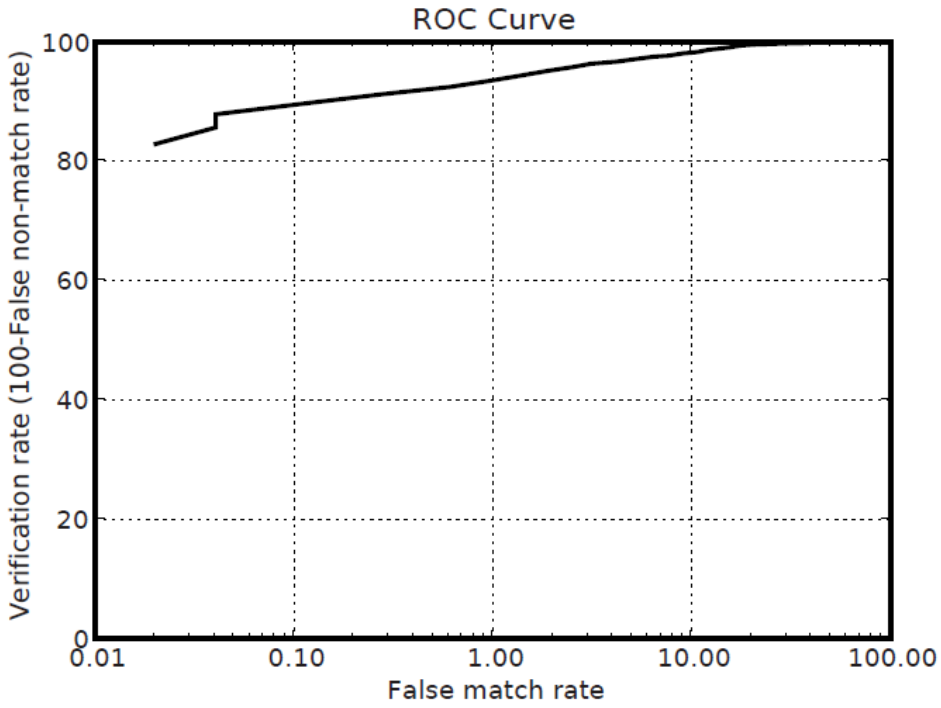


Figura 9 – Curva ROC [12]

Detection Error Trade-off (DET):

Muestran cómo varían las tasas de falsa aceptación, tanto FMR como FAR, frente a las de falso rechazo, FNMR y FRR

En el eje de abscisas se representa la FMR/FAR. En el de ordenadas, FNMR/FRR.

Puede verse un ejemplo en la figura 10.

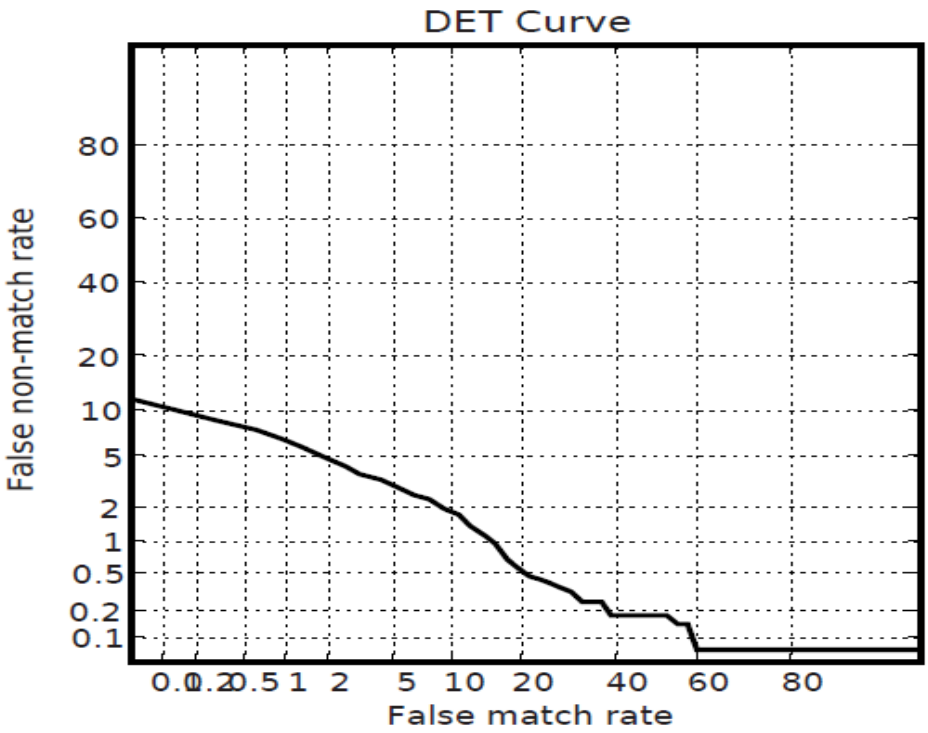


Figura 10 – Curva DET [12]

Cumulative Match Characteristic (CMC):

Muestra la tasa de identificación en función del rango. Figura 11.

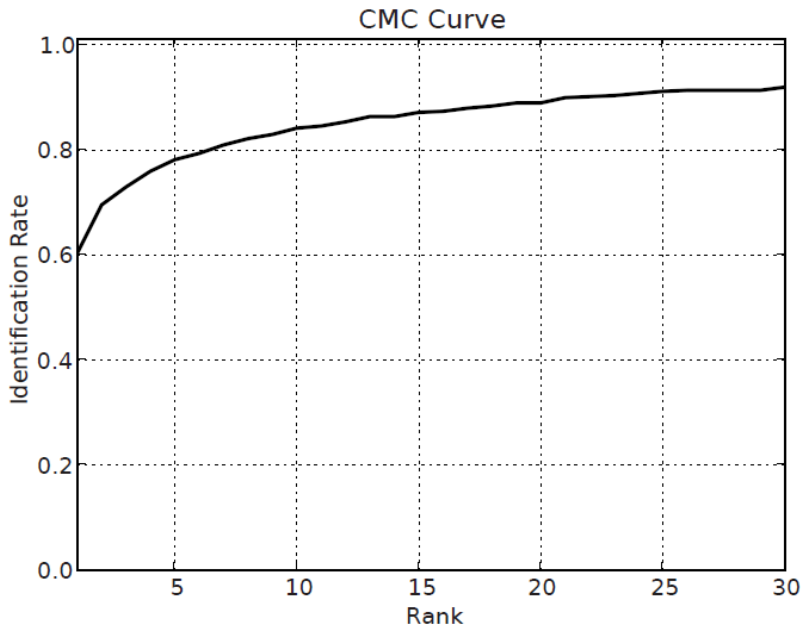


Figura 11 – Curva CMC [12]

Equal Error Rate (EER):

Es una representación de la curva FNMR/FMR o FRR/FAR. El punto en el que ambas tienen el mismo valor es donde se encuentra el EER. Figura 12.

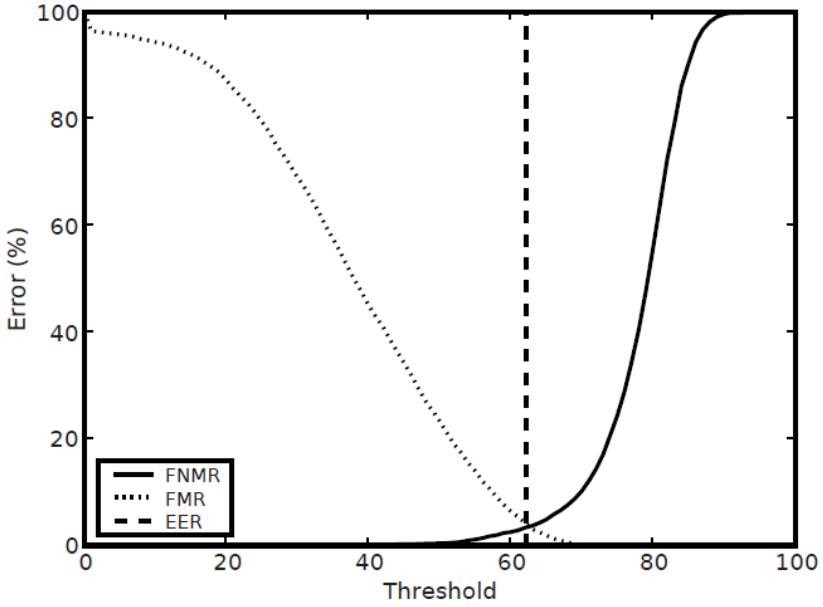


Figura 12 – Curva EER [12]

2.4.4. Interoperabilidad

Dado que este TFG trata la interoperabilidad de dispositivos de captura de huellas dactilares, resulta importante definir la interoperabilidad. La interoperabilidad es la habilidad de dos o más sistemas para intercambiar información y utilizar la información cambiada [13]. En el caso de las huellas dactilares se trata de evaluar el rendimiento al utilizar los patrones que han sido obtenidos en otros sistemas biométricos.

Como resulta entendible, las organizaciones que utilizan este tipo de dispositivos no siempre utilizarán exactamente los mismos. Al utilizar los datos obtenidos por un sensor con otro surgían problemas. Por ello es por lo que se comenzaron a realizar los estudios de interoperabilidad. Se comenzó a observar que no se conseguían los mismos resultados con un sensor que con otro. Para que existiera un estándar, se decidió establecer unas normas de interoperabilidad para que eso no siguiera ocurriendo.

El motivo de la creación responde a dos motivos. El primero fue si los formatos propietarios obtenían un mayor rendimiento cuando se trataba de identificar a los usuarios que el rendimiento que obtenían los formatos estándar. El segundo fue si era posible conseguir el mismo rendimiento en un sensor si las muestras que se comparaban habían sido generadas en otro sistema distinto [14].

En este trabajo se tratará el caso en el que los dispositivos son distintos. Se compararán dos tecnologías, la óptica y la capacitiva. Para ello se probarán todas las combinaciones entre ambos dispositivos, se verá más adelante, en el capítulo 5.

2.4.5. Evaluación de usabilidad y aceptabilidad

La definición que se usa de usabilidad viene dada por tres factores: la efectividad (precisión y éxito), la eficiencia (relación entre grado de éxito y los recursos gastados en conseguirlo) y la satisfacción (actitud positiva del usuario hacia el uso del sistema). Éstos tres factores son los que se han de tener en cuenta a la hora de crear un sistema que goce de verdadera usabilidad para el usuario.

Existe claramente relación entre usabilidad y seguridad. Éstos son dos factores fundamentales de un sistema pero se contraponen el uno al otro y dan lugar a distintas maneras de desarrollar dicho sistema [15].

Para resolver esta contraposición, se necesita realizar un diseño centrado en el usuario, más que a que se hace normalmente, centrarse en los problemas del interfaz en sí.

Es vital conocer la satisfacción de los usuarios en cuanto al sistema que han utilizado. Cada sistema biométrico tendrá unos parámetros distintos según los cuales medirá el grado de usabilidad y aceptabilidad.

En estas evaluaciones no se puede tener en cuenta todas las opiniones. Se ha de tener en cuenta las características de los usuarios según el tipo de usuario que vaya a tener el sistema finalmente. Un ejemplo podría ser un sistema de reconocimiento facial que vaya a ser utilizado por población caucásica no deberá ser testado por usuarios de color. Del mismo modo, las tasas de rendimiento y las de satisfacción no serán iguales para unos y para otros.

Es también de gran importancia evaluar el entorno en el que se va a implementar el sistema. Se ha de valorar el comportamiento de los usuarios que tendrá para poder realizar una implantación que sea verdaderamente útil para ellos. Suponiendo una nave industrial en la que los operarios transportan cajas de una parte a otra a través de varias salas, un dispositivo de huellas dactilares no sería el sistema más adecuado. Al tener las dos manos ocupadas con la caja, el operario se vería obligado a soltar la caja cada vez que desee atravesar una puerta. Esto crearía el rechazo del sistema y se llegarían a soluciones que echarían a perder la implementación del sistema de reconocimiento biométrico, como podría ser el bloquear las puertas con cajas para no tener que abrir y cerrar cada vez. Esto resultaría en un sistema útil implantado en un entorno que no es el adecuado y a la falta de seguridad que ello conlleva. En estos casos sería mejor pensar de antemano en el entorno e implantar otro tipo de sistema, un reconocimiento facial por ejemplo.

Para que esto no ocurra, es muy importante que las evaluaciones se hayan llevado a cabo sabiendo cómo es, tanto el entorno en el que se va a implantar, como los usuarios que van a hacer uso del sistema.

En cuanto a medidas de usabilidad contamos con una segmentación de los errores de tipo FTA (Failure to Acquire). Se dividen en dos posibles circunstancias, presentación errónea o presentación correcta Se explican los estos errores a continuación y puede encontrarse una descripción más gráfica en la figura 13.

1. Presentación errónea:

    i. Defective Intercactions (DI): El sistema no es capaz de detectar la característica del usuario.

    ii. Concealed Interactions (CI): El sistema detecta y la acepta como buena (Aun siendo una presentación errónea).

    iii. False Interactions (FI): El sistema detecta la muestra pero la clasifica correctamente como errónea.

2. Presentación correcta:

    i. Failure to Detect (FTD): El sistema no es capaz de detectar la característica biométrica del usuario (Aun siendo una presentación correcta).

    ii. Failure to Extract/Process (FTX/FTP): El sistema acepta la muestra pero no es capaz de procesarla.

    iii. Successful Processed Sample (SPS): El sistema detecta la muestra y la procesa correctamente.

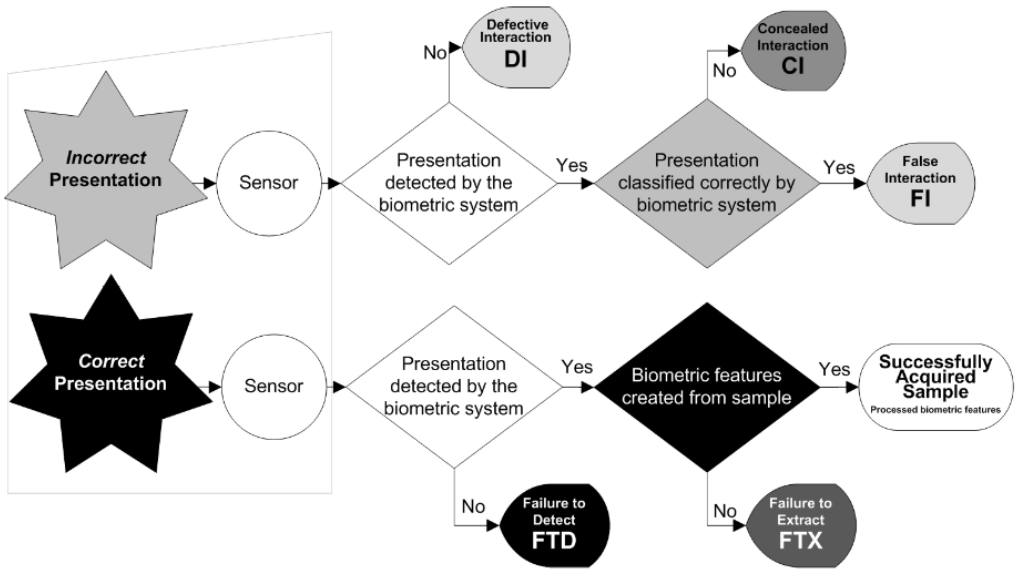


Figura 13 – Errores según presentación [16]

Una vez se ha dado una visión general acerca de la biometría, sus modalidades y los tipos de análisis, es momento de definir con más claridad de lo que trata este TFG.

El proyecto tiene como finalidad realizar un estudio de la interoperabilidad de dos sensores de distinta tecnología, óptica y capacitiva. Además se ha realizado un análisis de usabilidad de estos todos los sensores para poder relacionar interoperabilidad y usabilidad con el rendimiento, que es lo que indica cómo funcionan los sistemas y su grado de seguridad. El punto principal es reconocer qué tecnologías funcionan mejor cuando se les suministra una muestra de un sensor de tecnología distinta para realzar su propia identificación.

3. DISEÑO DEL SISTEMA DE EVALUACION

3.1. Diseño de la aplicación

Teniendo en cuenta que el objetivo es estudiar la interoperabilidad y la usabilidad de los sensores, surgen ciertos requisitos que han de ser satisfechos para que estos análisis sean útiles y sean realizados de manera adecuada.

Se detalla a continuación las especificaciones de diseño y las herramientas necesarias para cumplir todas ellas, tanto de software como de hardware.

3.1.1. Requisitos genéricos y específicos

Los dos objetivos principales de este TFG, análisis de interoperabilidad y análisis de usabilidad, obligaron a usar aplicaciones para poder explotar la BBDD que contenía las muestras. Para cumplir los requisitos que estos objetivos marcaban se debían identificar primero. De este modo se sabría qué aplicaciones poder desarrollar y como rralizar todo el estudio.

Se contaba con una de las aplicaciones, la que se encargaba de las tasas de rendimiento para la interoperabilidad, en cambio, la segunda tuvo que ser creada. Ambas fueron diseñadas en el programa MATLAB. Utilizando las GUI para realizar una interfaz más sencilla e intuitiva a la hora de extraer resultados.

- Obtención de usabilidad

  Con esta aplicación, se es capaz de cruzar todos los parámetros que contiene dos archivos log (apartado 3.1.1.3) que se sacaron a la hora de la creación de la BBDD. Esto es necesario para un mejor estudio de todos los factores que pueden llegar a afectar al uso de un dispositivo de huella dactilar.

Además de los requisitos meramente técnicos, se debió cumplir también requisitos legales como se ha comentado con anterioridad. Tanto con las normas ISO/IEC como con la LOPD. La información personal de los usuarios se guardó sin vincular directamente a los resultados que se obtuvieron de ellos. Mediante un número de usuario se vinculaban estos datos personales a estos resultados. Pero nunca de manera directa. Todo esto acorde a la LOPD.

Se debieron tener en cuenta aquellos factores que iban a afectar a cada análisis para hacerlo de la mejor manera posible. Además se desarrolló la aplicación de modo que fuera reutilizable para futuros proyectos.

3.1.1.1. Análisis de usabilidad

A la hora de desarrollar esta aplicación se debían tener en cuenta todos los parámetros que se encontraban en el archivo log. De este modo podría estudiarse todas las combinaciones de parámetros que se deseen para hacer el análisis más específico. Entre estos parámetros se encuentran:

- **Sensores:**

Se emplearon cuatro sensores cuyas características se detallarán más adelante (apartado 3.2.2). Cada uno tiene su modo de empleo y una tecnología distinta.

- **Dedo**

Como se verá más adelante, es importante tener en cuenta qué dedo se utilizó cuando ocurrieron los errores para poder evaluar de manera correcta si la elección del dedo utilizado afecta a la aparición de errores.

- **Visita**

A medida que avanzan las visitas, los usuarios empiezan a estar cada vez más familiarizados con el uso de los sensores. Por ello, no deberían ocurrir el mismo número de sensores.

- **Errores**

Debido a distintos usos erróneos de los usuarios, surgen distintos errores a la hora de procesar la muestra. De igual modo, es posible que la interacción del usuario con el sensor haya sido correcta pero haya habido algún problema con el procesado de la imagen que dé lugar a un error. Es por ello que se debe ser capaz de diferenciar cada tipo de error.

- **Sexo**

Un parámetro que es muy diferenciador y podría dar resultados interesantes.

- **Lateralidad (Diestro o zurdo)**

A la hora de utilizar un sensor es de gran importancia saber si su diseño crea algún tipo de inconveniente a los usuarios de una lateralidad concreta.

- **Edad**

Es sabido que las personas mayores son más propensas a tener problemas con las nuevas tecnologías por lo que se debe estudiar si hay algún sensor que resulte más interesante para distintos rangos de edad.

3.1.1.2. Reutilización de código

Con el objetivo de que la aplicación sea reutilizable y versátil, se deberá permitir al usuario elegir el archivo que desea abrir. De este modo no se limitará la aplicación a sólo unos usos, podrá ser usada de nuevo en otros proyectos similares.

3.1.1.3. Archivos log

De la aplicación utilizada en el reclutamiento (se verá en detalle en el apartado 3.2.1) y en las visitas, se obtuvo una BBDD que constaba de imágenes de las huellas dactilares. Paralelamente, la aplicación generó dos archivos log que se encargaban de registrar los eventos que sucedían durante la toma de muestras. Ambos archivos log se relacionan entre sí mediante el número de usuario que se daba a cada persona que se incluía en el sistema. Es decir, ambos contienen datos de los mismos usuarios, pero estos datos varían de un archivo a otro.

Los dos archivos log se almacenan en hojas Excel. De ellos se obtiene cierta información interesante acerca de los voluntarios que dieron sus muestras.

- Hay un total de 70 usuarios
- El género más presente es el masculino (76%) frente al femenino (24%).
- La distribución de edad es la siguiente
    - 70% menores de 30 años.
    - 23% entre 50 y 70 años.
    - 7% mayores de 50 años.
- Hay un 87.5% de diestros frente a un 12.5% de zurdos.

Debido a que esta BBDD y este archivo log fueron realizados en el entorno universitario, las muestras provienen de un grupo de usuarios que comparten gran parte de los rasgos. Es por ello que en el apartado 6 se proponga la creación de una BBDD con muestras provenientes de usuarios más dispares entre sí.

Estos archivos log son los que se utilizarán luego para el análisis de usabilidad.

3.1.1.3.1. Log 1

Se puede observar en la tabla 2 una porción del primer archivo log y de cómo se organizan los datos en él.

En esta primera hoja se encuentran guardados siete tipos de parámetros. Hora, fecha, número de usuario, sensor, dedo, visita y errores. En la aplicación que se desarrolla con este TFG es donde se decidirá de qué manera tratar todos estos datos.

Tabla 2 – LOG 1

Hora	Fecha	Nº de usuario	Sensor	Dedo	Visita	Errores			
17:10:28	21/02/2013	20005	O1	CD	R	SPS	SPS		
17:11:40	21/02/2013	20005	O1	PD	R	SPS	SPS		
17:12:10	21/02/2013	20005	O1	CI	R	SPS	SPS		
17:12:25	21/02/2013	20005	O1	PI	R	SPS	SPS		
17:12:43	21/02/2013	20005	O1	II	R	SPS	SPS		
17:13:03	21/02/2013	20005	LR	CI	R	SPS	FTD	FTD	SPS
17:14:01	21/02/2013	20005	LR	PI	R	SPS	FTD	SPS	
17:14:39	21/02/2013	20005	LR	II	R	SPS	SPS		
17:14:57	21/02/2013	20005	LR	PD	R	FTD	FTD	SPS	SPS
17:15:37	21/02/2013	20005	LR	ID	R	SPS	SPS		
10:12:19	22/02/2013	20006	LP	MD	R	SPS	FTX	SPS	
10:16:51	22/02/2013	20006	CS	II	R	SPS	SPS		

Para entender lo que significan estos datos es necesario explicar el significado de todas estas siglas.

- **Sensores:**
  - O1: Sensor óptico 1.
  - O2: Sensor óptico 2.
  - CS: Sensor capacitivo tipo swipe.
  - LR: Sensor óptico de huella rodada.
  - LP: Sensor óptico de huella posada.

- **Dedo:**
  - PD: Pulgar derecho.
  - ID: Índice derecho.
  - CD: Corazón derecho.
  - PI: Pulgar izquierdo.
  - II: Índice izquierdo.
  - CI: Corazón izquierdo.
  - MD: Mano derecha.
  - MI: Mano izquierda.

- **Visita:**
  - R: Reclutamiento.
  - V1: Visita 1.
  - V2: Visita 2.
  - V3: Visita 3.

- **Errores**:
  - SPS: Succesful Processed Sample.
  - FTD: Failure to Detect.

- FTX: Failure to Extract
- CI: Concealed Interactions.
- DI: Defective Interactions.
- FI: False Interactions.

3.1.1.3.2. Log 2

En el segundo archivo se almacenan unos parámetros distintos a los del primero. Estos datos son de gran importancia ya que resultan necesarios para poder hacer una criba de las muestras que han presentado todos los usuarios. Son parámetros muy relevantes para los análisis de usabilidad. Los parámetros son el sexo del usuario, su edad o la lateralidad, tabla 3.

Tabla 3 - LOG 2

Nº	M/F	D/Z	Edad	Dedos mutilados
20001	M	D	29	False
20002	F	D	32	False
20003	F	D	21	False
20004	F	D	25	False
20005	M	D	22	False
20006	M	D	22	False
20007	M	D	28	Corte pulgar izq.
20008	M	D	25	False
20009	F	D	52	False
20010	M	D	32	False
20011	M	Z	21	False
20012	M	Z	22	False
20013	M	D	32	False
20014	M	D	32	False
20015	M	D	28	False
20016	M	D	22	False
20017	M	D	23	False
20018	M	D	22	False
20019	M	D	25	False
20020	F	D	21	False
20021	M	D	23	False
20022	M	D	45	False

- **Sexo:**
  - M: Masculino.
  - F: Femenino.

- **Diestro Zurdo:**
  - D: Diestro.
  - Z: Zurdo.
- **Edad:**
  - La edad, en número entero.

Como se puede apreciar, y se ha comentado anteriormente, los dos archivos están únicamente relacionados mediante el número de usuario, protegiendo así los datos de los voluntarios. Además de todo esto, el número de usuario no se puede asociar a la identidad de los voluntarios que dieron sus huellas dactilares, consiguiendo así más privacidad.

3.2. Herramientas utilizadas

Para la realización de todos los requisitos antes mencionados, se ha contado con una serie de software y de hardware. El software constaba de la BBDD y la aplicación que capturo las muestras, además se utilizó MATLAB para la elaboración de la aplicación de usabilidad. En cuanto al hardware, se contaba con equipos y sensores.

3.2.1. Aplicación para la creación de la BBDD

El proceso que se llevó a cabo para la captura de la BBDD era siempre el mismo para cada usuario

El operario se debía asegurar de que todos los aspectos de la evaluación estaban claros para el usuario. Además debía mostrarle todos los sensores para que se familiarizara con ellos y explicar todo lo que se iba a hacer en esa y en las visitas sucesivas. El operario se aseguraba de que el proceso estuviera claro y de que el usuario supiera que su identidad y las imágenes de sus huellas no iban a estar relacionadas y que estarían protegidas por la LOPD.

Al tomarle los datos al usuario, también se recogía información que sería pertinente a la hora de analizar los resultados, el formulario se puede ver en la figura 14. La edad, el puesto de trabajo, la lateralidad (diestro o zurdo) o las mutilaciones son factores que pueden afectar en gran manera a las huellas dactilares.

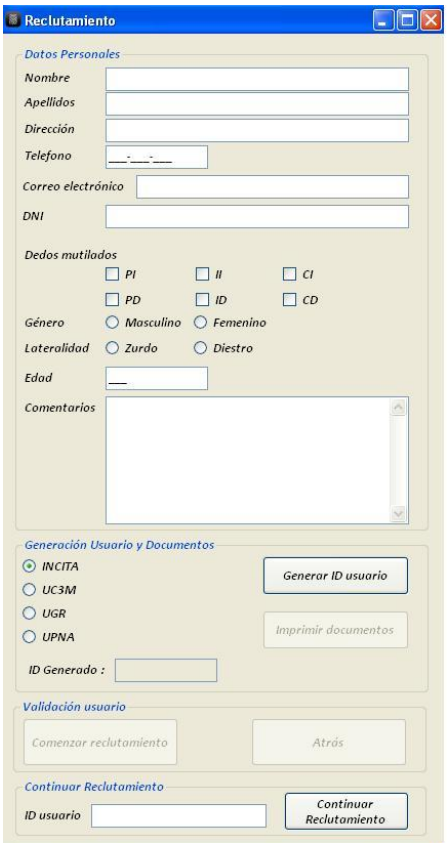


Figura 14 - Formulario

3.2.1.1. Capturas

En esta etapa del proceso se obtenían las muestras de todos los usuarios para la BBDD. Se puede dividir el proceso en dos etapas: Reclutemiento y reconocimiento.

3.2.1.1.1. Reclutamiento

Antes de explicar en qué consistía el reclutamiento y el reconocimiento, se ha de aclarar que no se tomaban los cinco dedos de cada mano. Sólo se obtenían muestras de pulgar, índice y corazón de ambas manos.

En el reclutamiento se necesitaba sólo una buena huella pero debía tener una calidad aceptable. Esto es debido a que el resto de las muestras se iban a comparar con esta primera. Si esta fallaba, todas las siguientes darían error aunque estuvieran bien tomadas ya que estarían comparándose con una huella que no es correcta y por lo tanto daría lugar a un error

En cuanto a la calidad de la huella, en la aplicación utilizada existía un apartado en el que se podía ver la imagen. Figura 15. En la parte de debajo de esta imagen apetecía un número del 1 al 5, siendo 1 la mejor calidad y 5 la peor, que ayudaba a decidir si la imagen era suficientemente buena.

Figura 15 – Verificación de calidad de la huella

3.2.1.1.2. Reconocimiento

Tras el reclutamiento, y aun dentro de la primera visita, se realizaba la primera identificación. Este proceso es prácticamente igual que el de reclutamiento exceptuando que el número de muestras necesarias y los intentos para cada muestra varían.

Pasadas dos semanas el usuario puede volver a realizar la segunda visita que consta únicamente de un reconocimiento. Es exactamente igual que el proceso realizado durante la última parte de la primera visita. En estos reconocimientos, la captura de las huellas no seguía siempre el mismo orden en los dedos, lo que causó la aparición de ciertos problemas que se comentarán en el análisis de usabilidad, apartado 5.

Pasada una semana más, se puede realizar la tercera y última visita, que es exacta a la segunda.

3.2.2. Equipo y sensores para la creación de la BBDD

El material consistía en dos equipos completos de toma de huellas dactilares. Cada uno de ellos constaba de:

- Un PC con el software instalado
- 4 sensores de huellas dactilares

Los sensores utilizados fueron:

Sensor rodado/posado

Se trata de uno de los sensores ópticos con los que se contaba.

Este dispositivo, debido a su gran tamaño y peso (tabla 4), es difícil de manejar. Se utiliza de dos maneras distintas.

La primera de ellas se trata de apoyar simultáneamente los dedos índice y corazón. Para comenzar a tomar muestras la pantalla del sensor emite una luz verde, esta señal indica que ya se puede situar el dedo. Al situar los dos dedos en el sensor emite un pitido que indica que la muestra ha sido tomada y que se pueden retirar los dedos.

La segunda manera se trata de una huella rodada. En este caso, al escuchar el primer pitido el usuario debe rotar lentamente su dedo sobre su eje longitudinal hasta escuchar el pitido.

Se pudo observar que da una gran cantidad de problemas a la hora de realizar las huellas rodadas ya que se deben hacer con especial cuidado, teniendo en cuenta la rotación del dedo y la velocidad. Por ello es imprescindible que un operario supervise constantemente este sensor. Además a la hora de hacer la huella rodada, no es cómodo hacerlo ya que el giro de la muñeca no es el natural.

Tabla 4 – Características sensor rodado/posado

Conexión	USB 2.0
Área para la captura	48 x 48 mm
Resolución	500 dpi
Modo de captura	Posado dual / Rodado
Tipo de sensor	Óptico
Tamaño del dispositivo	84 x 171 x 63 mm

Figura 16 – Sensor rodado/posado

Sensor óptico 1

Este sensor es uno de los más rápidos a la hora de tomar muestras y captura la huella de un dedo cada vez.

El funcionamiento es muy simple. La pantalla del dispositivo se ilumina con una luz azul y en ese momento se puede colocar el dedo. Se debe dejar el dedo colocado en la pantalla alrededor de 2 o 3 segundos y la muestra será tomada en este intervalo de tiempo.

Tabla 5 – Características sensor óptico 2

Conexión	USB 2.0
Área para la captura	16 x 19 mm
Resolución	500 dpi
Modo de captura	Posado
Tipo de sensor	Óptico
Tamaño del dispositivo	66 x 90 x 58 mm

Figura 17 – Sensor óptico 1

Sensor óptico 2

Se trata de otro de los sensores ópticos.

Es otro sensor óptico que se utilizó para realizar las capturas de huellas dactilares.

Este sensor resulta muy sencillo de utilizar pero a su vez es lento a la hora de comparar la muestra.

La utilización consiste en posar sobre el área de captura un dedo cada vez. Al apoyar el dedo en la pantalla, ésta se enciende con un tono azul. Una vez apagada, se puede retirar el dedo ya que la muestra ha sido tomada correctamente.

Hubo ciertos problemas con algunos usuarios que al tener dedos demasiado grandes para la pantalla del sensor, no se podía ver como se apagaba esta luz por lo que no sabían con certeza si podían retirar el dedo o si la muestra aún no había sido tomada y debían dejar el dedo más tiempo.

Tabla 6 - Características sensor óptico 1

Conexión	USB 2.0
Área para la captura	16 x 18 mm
Resolución	508 dpi
Modo de captura	Posado
Tipo de sensor	Óptico
Tamaño del dispositivo	27 x 40 x 73 mm

Figura 18 – Sensor óptico 2

Sensor capacitivo

Este sensor, gracias a su pequeño tamaño resulta muy cómodo de utilizar pero debido a su pequeño área de captura surgen algunos problemas.

Es el único sensor capacitivo con el que se cuenta para el análisis y el único sensor de barrido (o swipe). Para utilizarlo se debe deslizar el dedo a lo lardo del dispositivo siguiendo unas flechas que lo hacen muy intuitivo de usar. Figura 19. Debido al

pequeño tamaño que tiene, el usuario puede cogerlo con sus propias manos y posicionarlo de manera que le resulte más cómodo.

El problema que se encuentra es que la pantalla es muy pequeña, tabla 7, y algunos usuarios, por falta de costumbre o de conocimiento, deslizan sobre la superficie de captura una porción demasiado pequeña del dedo, dando lugar a muestras con las que no se puede realizar comparaciones. Por esto, también es necesario que un operario ayude a los usuarios en este proceso de captura.

Tabla 7 – Características sensor capacitivo

Conexión	USB 2.0
Área para la captura	25 x 10 mm
Resolución	508 dpi
Modo de captura	Barrido
Tipo de sensor	Capacitivo, CMOS
Tamaño del dispositivo	84 x 34 x 14 mm

Figura 19 – Sensor capacitivo

3.2.3. Muestras

No todos los sensores capturan una muestra idéntica. Según el sensor que sea, se obtendrá una imagen u otra. Tabla 8. Por ello es importante que los sistemas sean capaces de identificar la muestra venga del sensor que venga, ya que pude ser que en una BBDD la imagen recogida provenga de un sensor distinto al que se está utilizando para obtener la muestra en ese instante. De aquí surge la interoperabilidad que se desea estudiar en este TFG.

Tabla 8 – Muestras de los distintos sensores

Óptico1	Óptico 2	Capacitivo	Posada	Rodada
				
				

4. Aplicaciones de captura y análisis de BBDD

En este capítulo se detallará la manera en la que se han cubierto las necesidades que el sistema requería para realizar análisis correctos y rigurosos. Además se comentará también la manera en la que se ha procedido para cumplir todos los requisitos que se han expuesto en el capítulo anterior.

Se contó con la aplicación básica para crear la base de datos que se ha detallado en el apartado 3.2.1. De aquí salen dos ficheros log que cumplen la norma de no vincular los resultados de errores a los datos personales de los usuarios.

Teniendo en cuenta estos dos ficheros, se desarrollará una GUI en Matlab que permita sacar datos objetivos de la usabilidad de los distintos sensores. Además de los distintos sensores, se podrá observar la usabilidad dependiendo de cualquiera de los parámetros contenidos en los ficheros.

4.1. Aplicación para el análisis de la BBDD

Para realizar el análisis de usabilidad, se ha creado una interfaz que permite analizar ambos ficheros log al mismo tiempo. Esto se ha realizado aprovechando el número de usuario.

Ya que lo que se va a realizar es un análisis de usabilidad, se han de tener en cuenta todos los parámetros y todas las combinaciones que sean posibles mediante el cruce de todos ellos. Se cuenta con varios parámetros que ya se han comentado con anterioridad pero sólo siete de ellos son interesantes para el análisis: Sensor, visita, dedo, diestro/zurdo, sexo, edad y tipo de error.

Para poder cruzar de una manera sencilla los siete parámetros se crea una aplicación GUI en Matblab. Puede verse la pantalla de diseño en la figura 20 y la aplicación final en la figura 21.

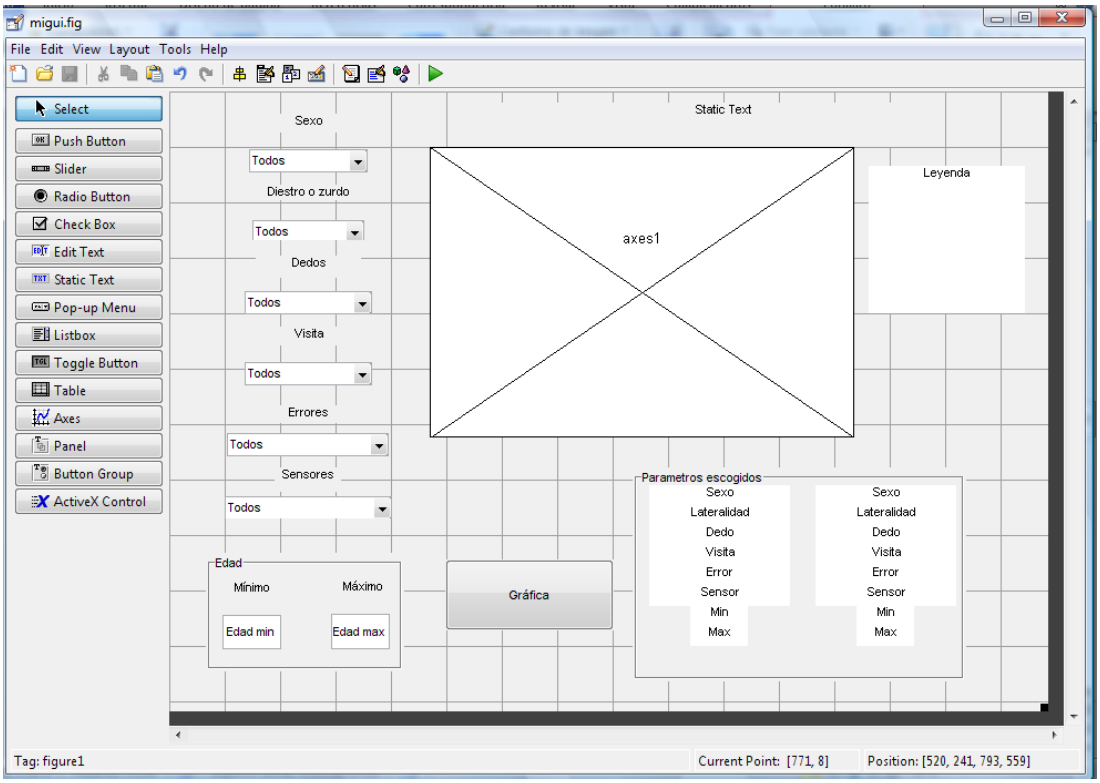


Figura 20 - Diseño de la GUI

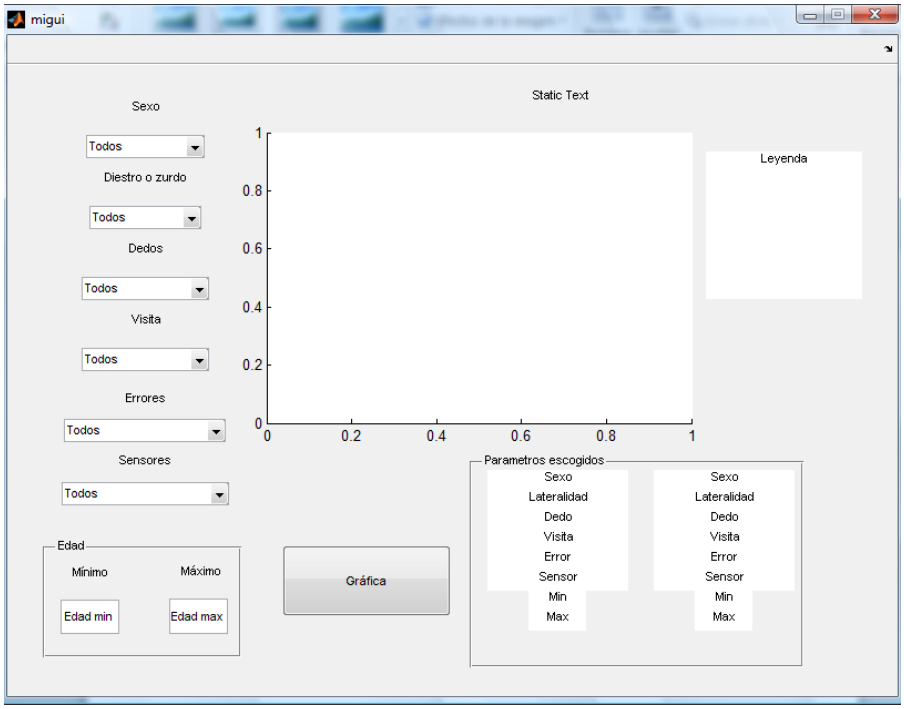


Figura 21 - GUI

La idea de este trabajo es analizar, mediante algunas de estas siete variables, la usabilidad de cada tipo de sensor. Es por ello que la interfaz permite escoger de entre todas ellas y entre todas las posibilidades que ofrecen mediante menús desplegables. Figura 22.

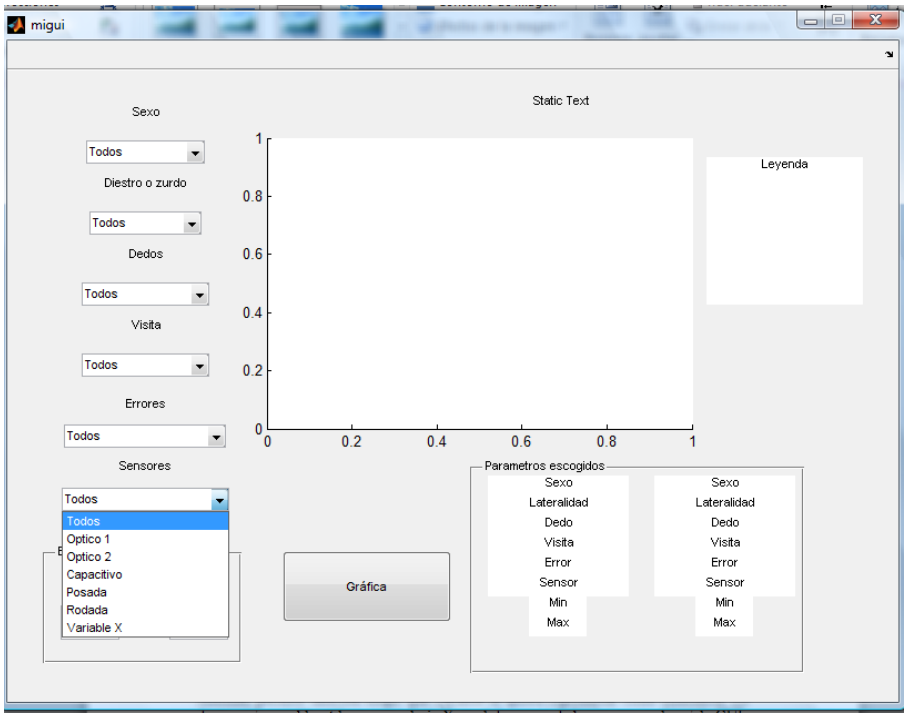


Figura 22 - Menús desplegables de la GUI

Además, permite también elegir qué variable se quiere representar como referencia. Es decir, qué variable utilizar para el eje X en el histograma que realizará la GUI. Con ello se logra poder adaptar el gráfico para que sea más sencillo de trabajar con los resultados. Figura 23.

Figura 23 - Selección de variable X

Tras elegir los parámetros, con sólo hacer click en el botón de 'Gráfica', nos aparecerá un histograma representando los parámetros que se he han elegido. Figura 24

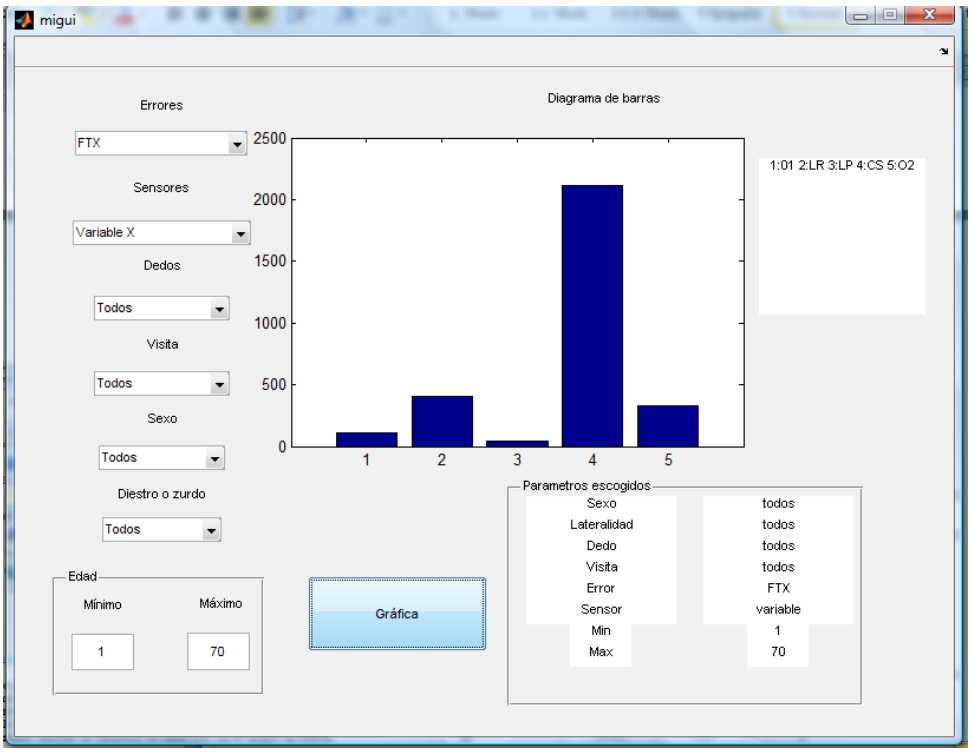


Figura 24 - Resultados en la GUI

Como se ha comentado en el capítulo 3, se ha decidido crear esta aplicación de modo que el usuario pueda decidir que archivo Excel desea abrir para hacerla reutilizable. Por ello, tras la selección de los parámetros, saltará una pantalla que indicará al usuario que

debe elegir el archivo que desea abrir como primer fichero log. Tras seleccionarla, se abrirá una segunda pantalla que repetirá la acción salvo que en esta ocasión será la segunda. Puede verse la manera en la que se da a elegir el archivo log en ambos casos en las figuras 25 y 26.

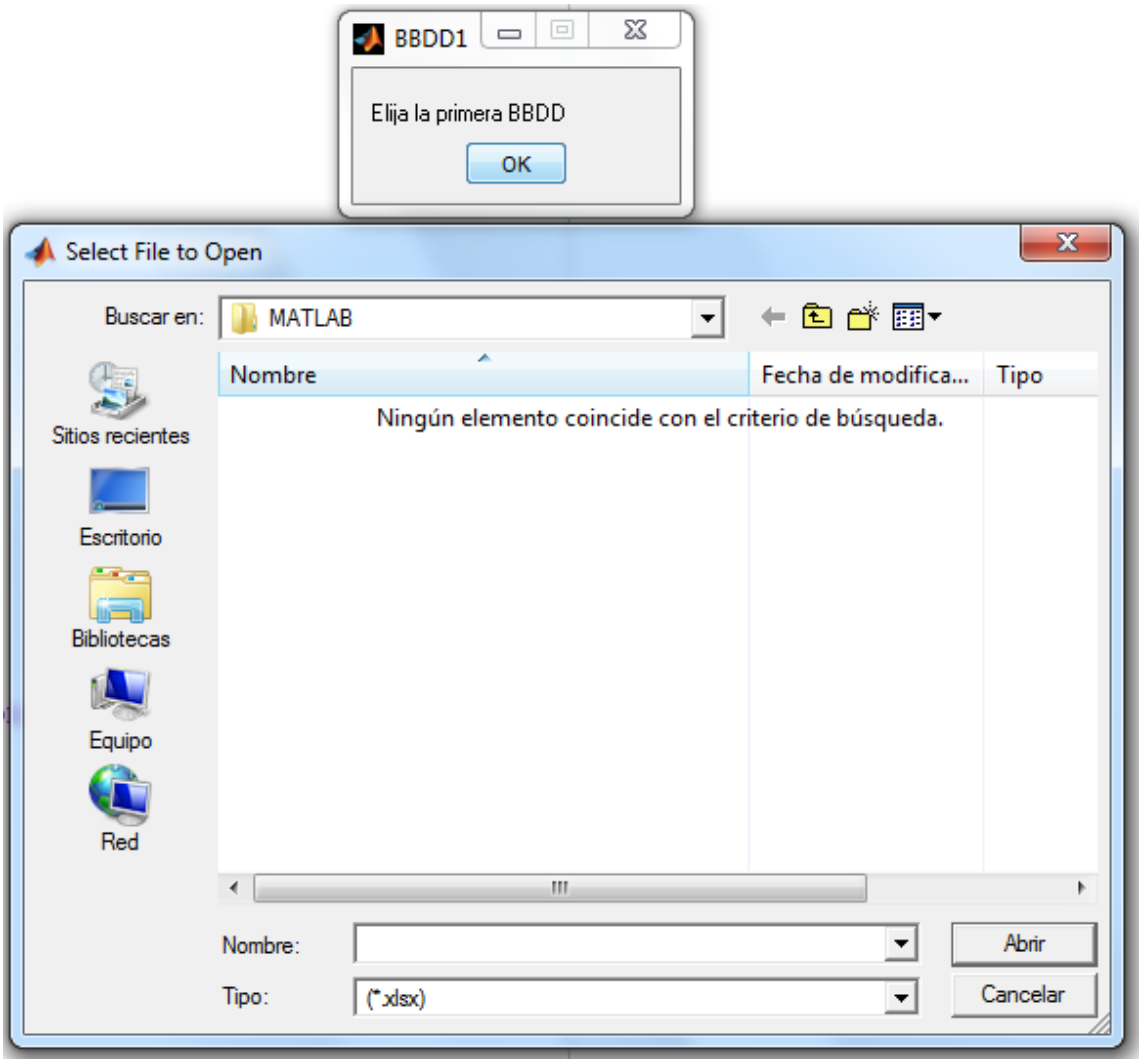


Figura 25 - Selección BBDD 1

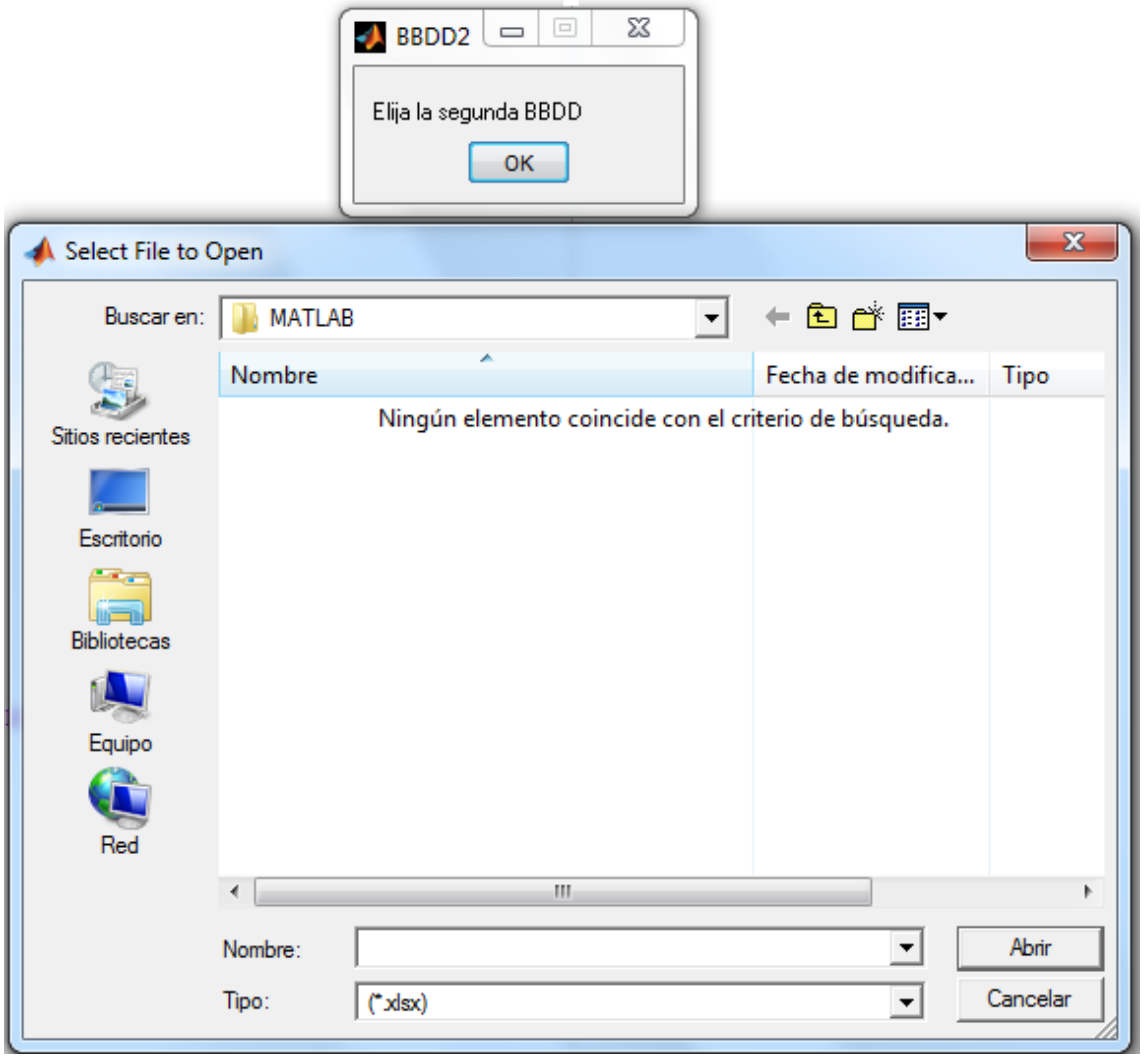


Figura 26 - Selección BBDD 2

Para tratar los datos, se realizan una selección dentro de las matrices de datos de modo que con cada iteración se analice un parámetro y se eliminen de la selección aquellas muestras de los usuarios que no cumplen con los parámetros. Para el final de las iteraciones, se tienen unas matrices que contienen las muestras que exactamente cumplen los requisitos de parámetros que el usuario ha elegido.

Teniendo esta selección de datos, se pasa a evaluar cuál es la variable que se ha elegido como 'variable para el eje X'. De este modo se contabilizan los datos según esta variable.

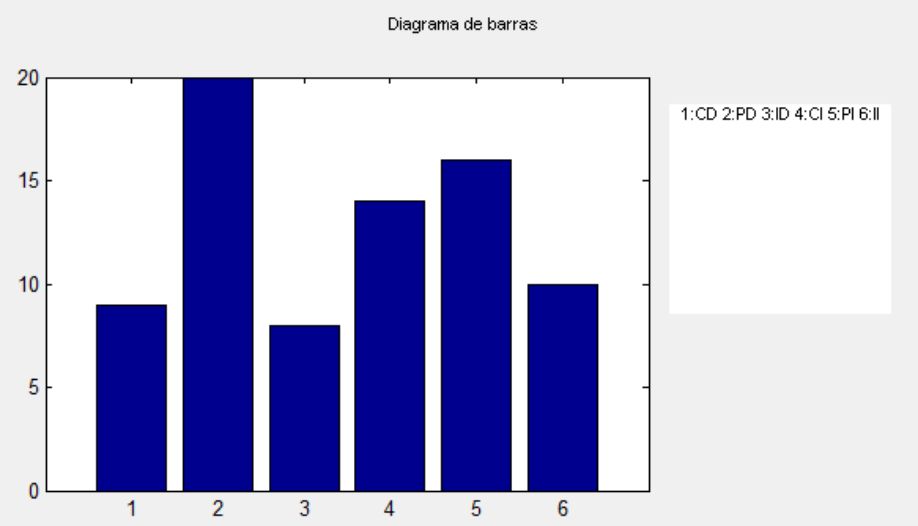


Figura 27 - Detalle eje x

Cómo puede verse en la figura 27, al haber seleccionado la variable ‘sensores’, éstos se sitúan en el eje X y se crea el histograma a partir de ahí.

Además genera una caja de texto que nos indica de qué variable depende cada una de las barras del histograma. Figura 28.

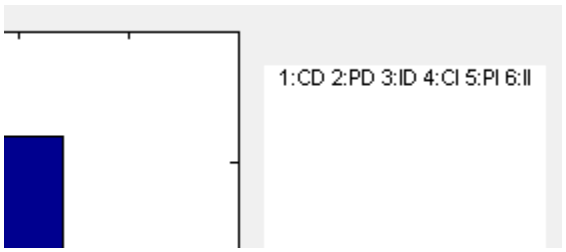


Figura 28 - Leyenda para el eje x

Se crea también una leyenda en la que se pueden observar las elecciones de parámetros que ha hecho el usuario. Figura 29.

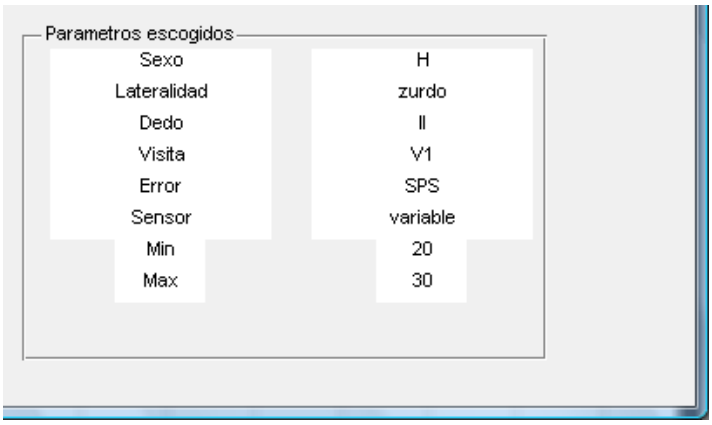


Figura 29 - Parámetros escogidos

Ha de tenerse en cuenta que es posible que alguna de las combinaciones elegidas no existan. Se ha contemplado esta posibilidad y el programa emitirá un mensaje, como el que puede observarse en la figura 30, indicando que no hay datos que cumplan las condiciones.

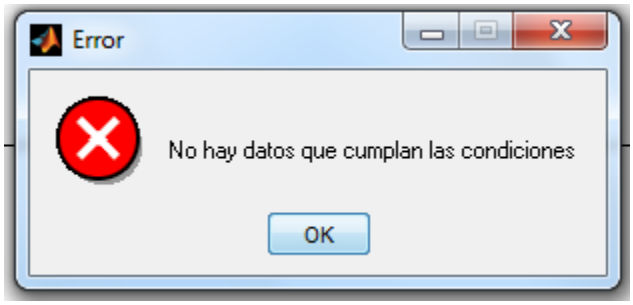


Figura 30 - Aviso

Ya que se pueden analizar todas las combinaciones de parámetros, se han elegido unas que dan un mejor reflejo de lo que se desea estudiar en este TFG.

4.2. Uso de la aplicación

El modo de empleo de la aplicación se ha diseñado de modo que sea lo más intuitivo y sencillo de usar posible.

El usuario deberá saber cómo quiere qué parámetros desea filtrar y cuál de ellos utilizar para el eje x. A modo de ejemplo se utilizará el evento SPS, con el sensor de huella rodada, con todos los dedos, de las mujeres diestras entre 23 y 33 años. Además se elegirá que en el eje x se sitúen el reclutamiento y las 3 visitas. Figura 31.

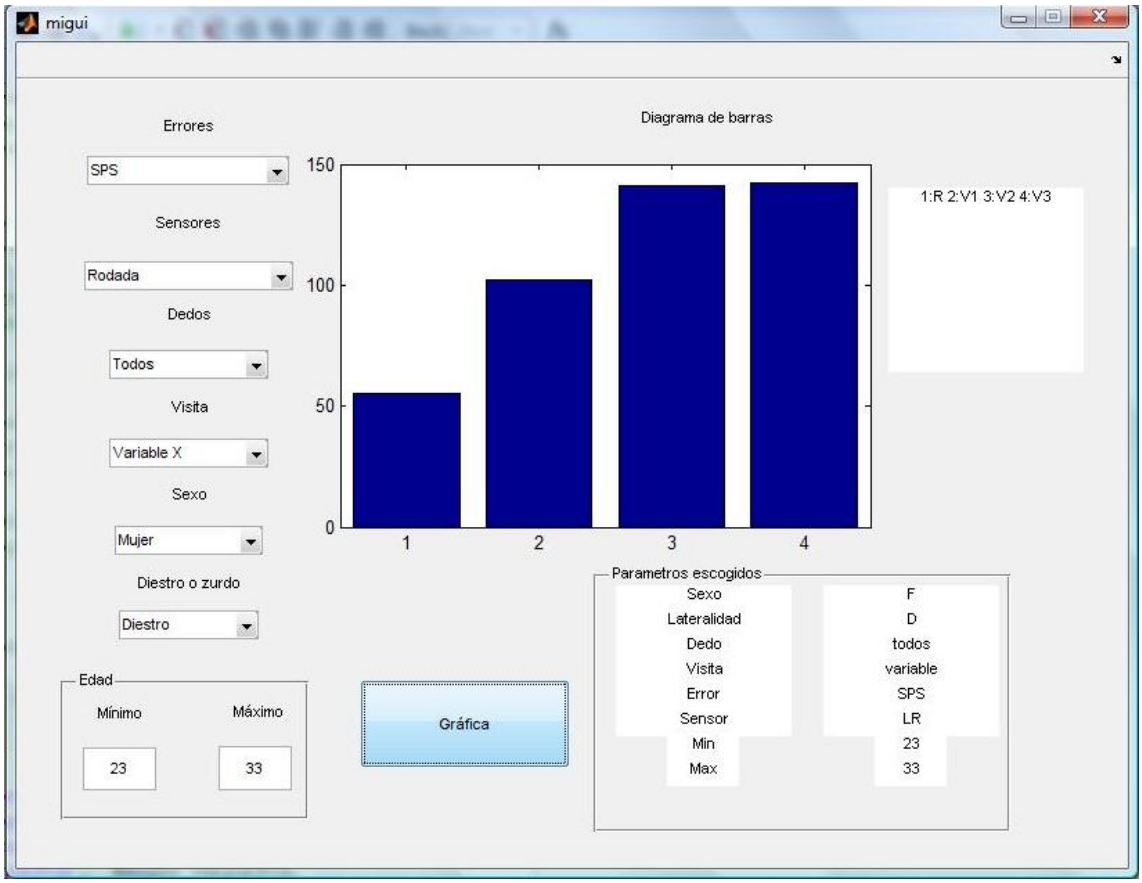


Figura 31 – Ejemplo de uso

De este modo se ve como aparece el histograma con las características que el usuario deseaba. En la parte inferior derecha aparecerá una leyenda en la que se indican los parámetros que se han elegido y a la derecha del histograma aparecerá la leyenda del eje x para aclarar a qué factor pertenece cada barra.

En el apartado 5 se verán los usos que se le ha dado a esta versatilidad de modo que se han podido segregar a los usuarios dependiendo de distintos parámetros que se han creído adecuados para el estudio

5. Estudios

En este apartado se recopilan y explican los resultados que se han obtenido a lo largo de todos los análisis explicados en los apartados anteriores.

Se tratará primero la interoperabilidad entre sensores ópticos y capacitivos y en segundo lugar la usabilidad de todos ellos.

5.1. Interoperabilidad entre sensores ópticos y capacitivos

En este primer análisis se compararán las tasas de rendimiento de dos sensores con distinta tecnología, se utilizará para ello el sensor óptico Biomini y el sensor capacitivo Eikon. En cada test se variará la combinación en el sensor en el que se ha realizado el reclutamiento y la verificación. Se tendrán en cuenta las 3 visitas para que los resultados sean más fiables.

5.1.1. Test 1

En este primer test se comparan los resultados que se obtienen al realizar el reclutamiento con un dispositivo óptico o capacitivo y la verificación con un sensor que utilice la misma tecnología. El esquema de este primer test pueden observarse de manera más visual en la Figura 32.

De este modo se obtiene unos resultados básicos con los que poder comparar cuando se obtengan los datos del test 2.

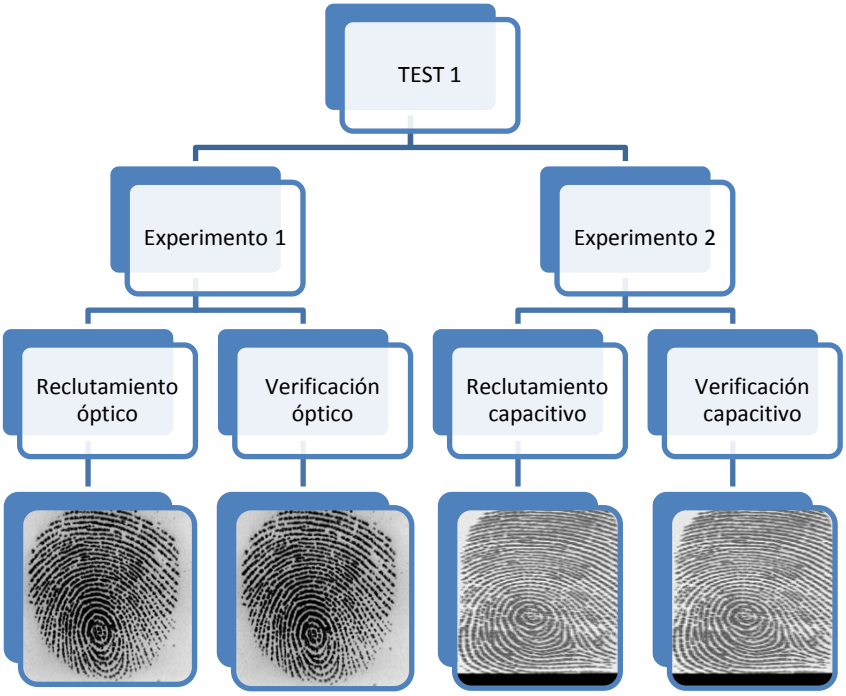


Figura 32 - Test 1

5.1.1.1. Resultados experimento 1

En la figura 33 se puede observar la curva FAR vs FRR para el primer experimento

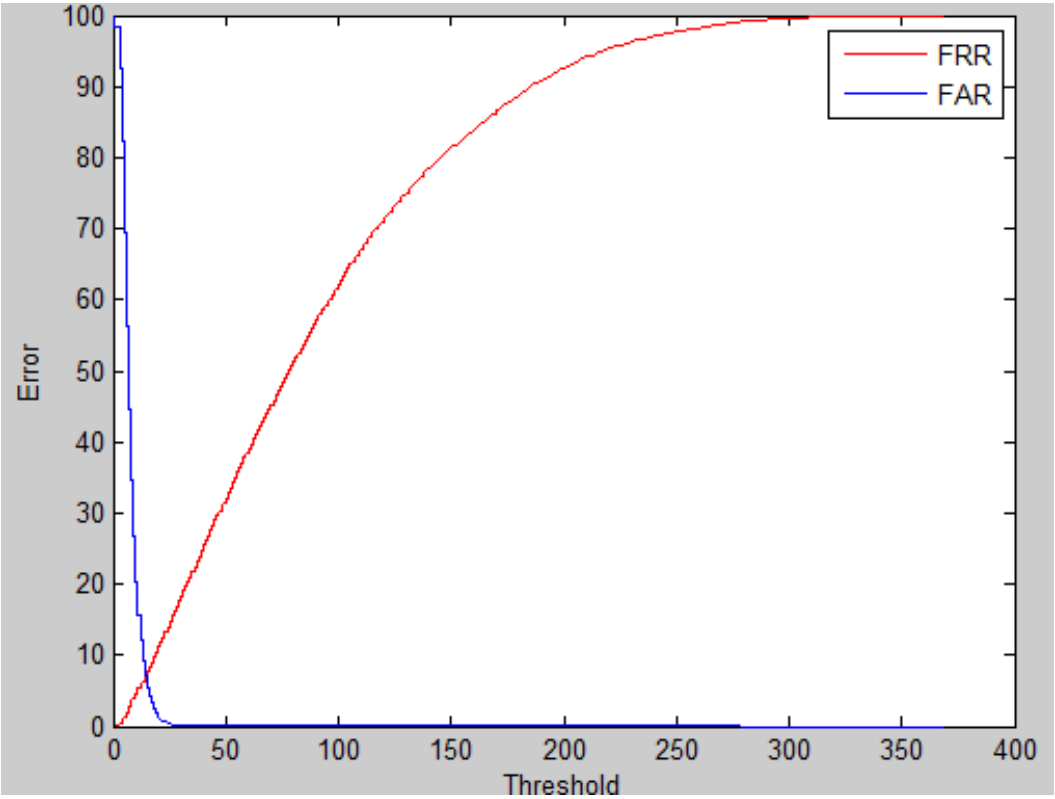


Figura 33 - Curva FARvsFRR para óptico

En este primer experimento se ha realizado tanto el reclutamiento como la verificación con un dispositivo óptico.

Como se ha explicado en el capítulo 2, el EER es el lugar en el que las dos curvas se cruzan, dando lugar a el punto en el que el sistema tiene mejor rendimiento. En este caso el EER tiene un valor de 9%.

5.1.1.2. Resultados experimento 2

En la figura 34 se puede observar la curva FAR vs FRR para el segundo experimento

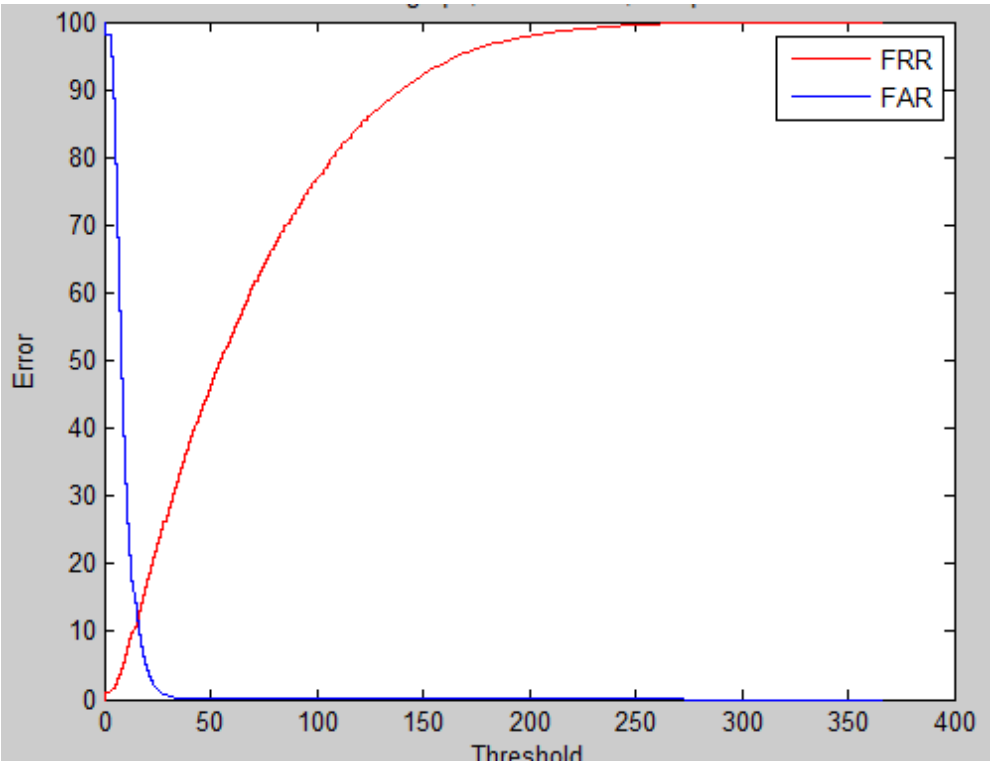


Figura 34 - Curva FARvsFRR para capacitivo

En este segundo experimento se ha realizado tanto el reclutamiento como la verificación con un dispositivo capacitivo.

En este caso el EER tiene un valor de 13%.

Puede verse que el rendimiento del sensor capacitivo es menor. Esto puede deberse al mal uso que hacían de él los usuarios y a que la superficie de captura de huellas era mucho menor que en el caso del sensor óptico.

5.1.1.3. Resultados test 1

Se presentan ahora las curvas ROC y DET del primer test.

En la figura 35 se puede observar la curva ROC cuando el reclutamiento y la verificación se han realizado son un sensor óptico (azul) y cuando se han realizado con sensor capacitivo (rojo).

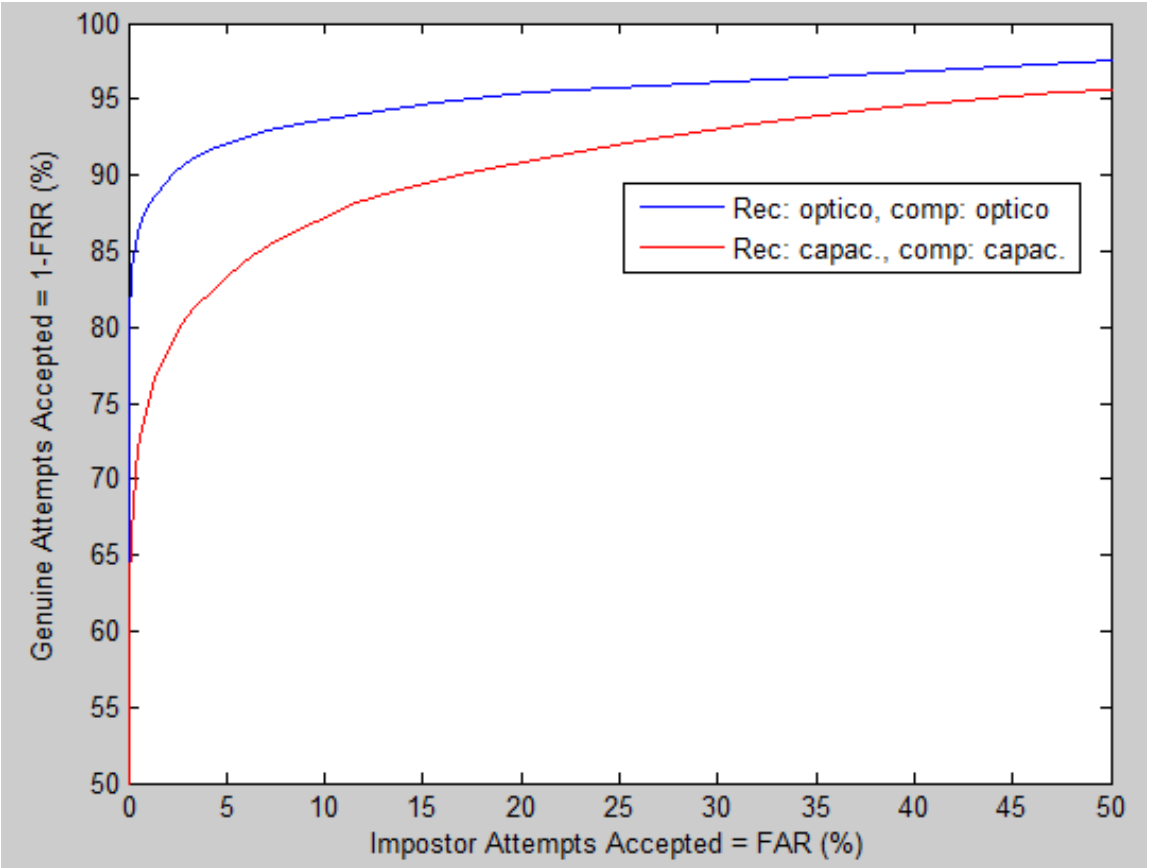


Figura 35 - Curva ROC test 1

Ni con el sensor capacitivo ni con el óptico se alcanza la curva ideal. Cuando el FAR es del 0% (corte con el eje de ordenadas), el sensor capacitivo es del 86% y el óptico es del 92%. Ya que el óptico se acerca más a la curva ideal, confirmamos lo visto en el anteriormente, el sensor óptico tiene mejor rendimiento.

En la figura 36 se puede observar la curva DET para este test. La curva roja vuelve a ser para el sensor capacitivo y la azul para el sensor óptico.

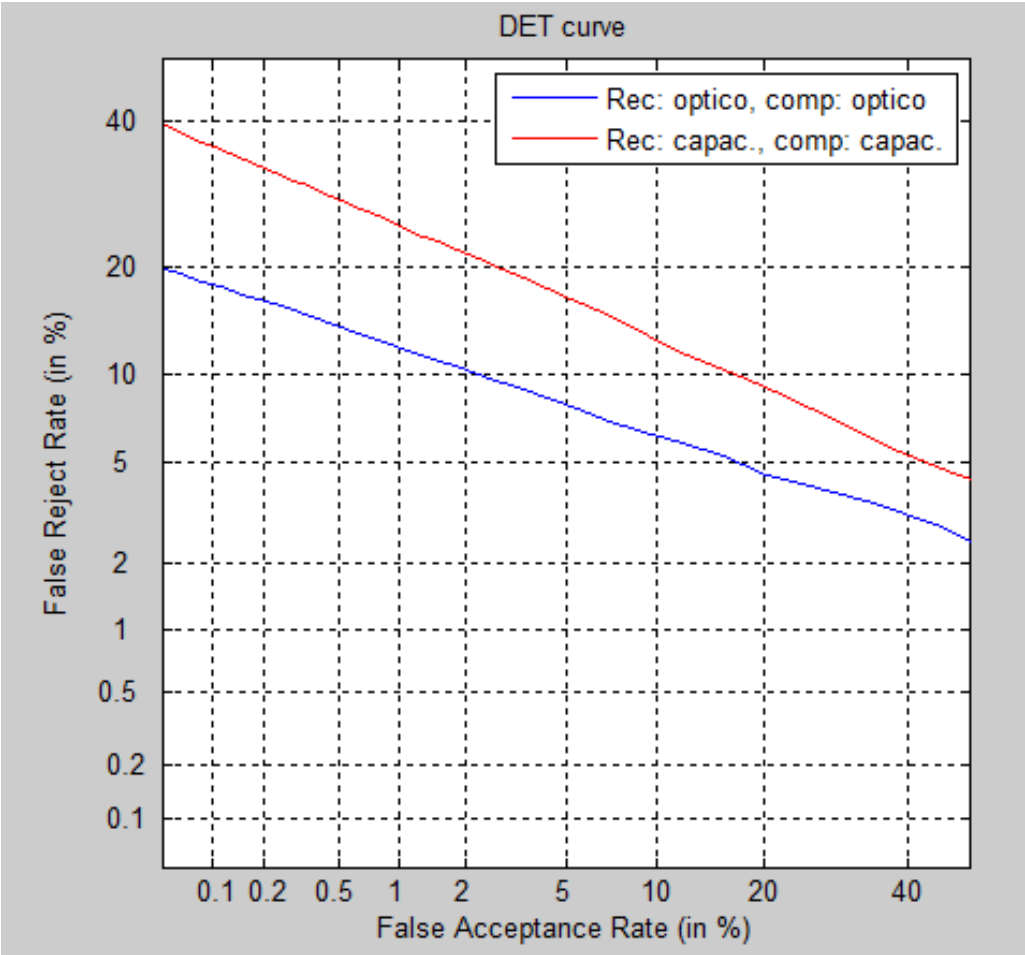


Figura 36 - Curva DET test 1

Al comparar estas dos curvas casi lineales con la curva ideal del rendimiento de un sistema biométrico, se observa que quedan lejos de coincidir.

Aun así podemos observar como el mejor rendimiento es para el sensor óptico ya que corta por debajo de la curva del sensor capacitivo, en el eje de ordenadas. Verificando de nuevo los resultados de los apartados anteriores.

Esta gráfica permite comparar ambos valores de EER. Si se traza una recta Y=X, allí donde corte con las curvas, será el EER. Puede compararse con los valores de las curvas FAR vs FRR viendo que coincide.

5.1.1.4. Conclusiones test 1

Se puede concluir que el sensor con mejor rendimiento es el óptico debido a su mayor superficie de adquisición de muestras. De modo que la muestra que se obtenía tenía más puntos característicos y de este modo se realizan comparaciones más precisas.

5.1.2. Test 2

En el test 2 se ha cruzado la manera de realizar la prueba. En la figura 37 se puede observar que en el primer experimento se ha realizado el reclutamiento con un sensor óptico y la verificación con un sensor capacitivo y en el segundo experimento se invierte, reclutamiento con sensor capacitivo y verificación con sensor óptico.

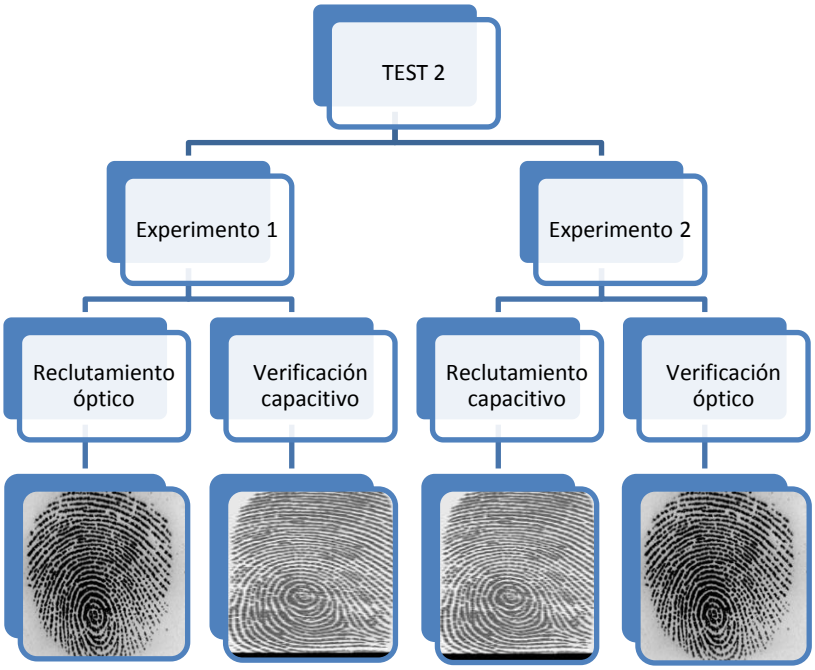


Figura 37 - Test 2

5.1.2.1. Resultados experimento 1

En la figura 38 se puede observar la curva FAR vs FRR para el primer experimento

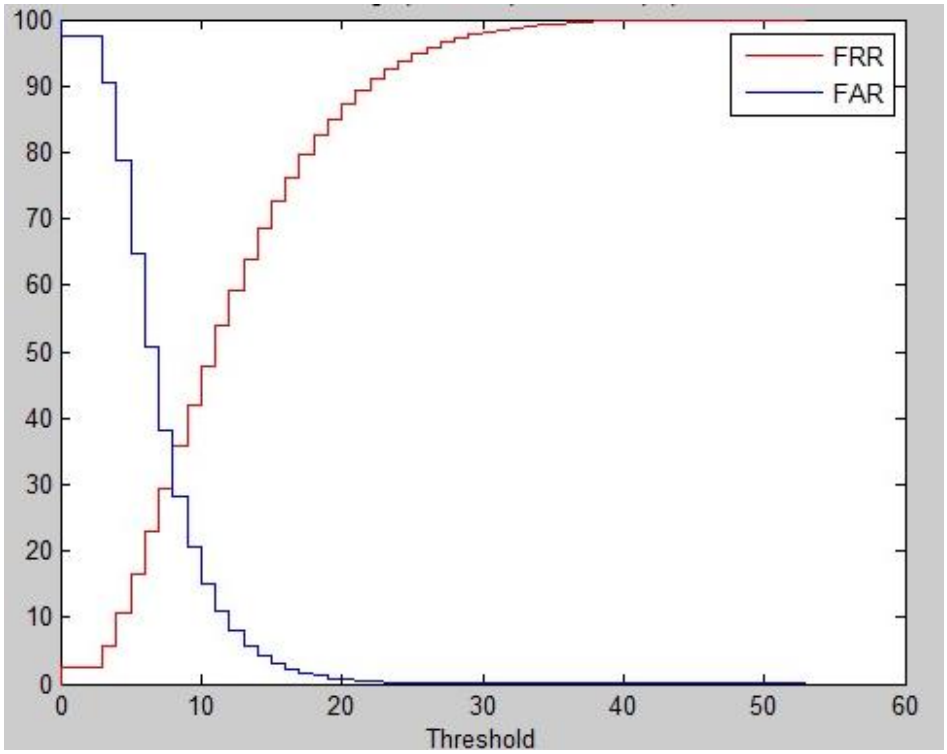


Figura 38 - Curva FARvsFRR para test 2, experimento 1

En este primer experimento se ha realizado el reclutamiento con un dispositivo óptico y la verificación con un dispositivo capacitivo.

En este caso el EER tiene un valor de 36%. Este es un valor mucho más elevado que cualquiera de los obtenidos en el primer test, dando indicios de una mala interoperabilidad entre ambos sensores.

5.1.2.2. Resultados experimento 2

En la figura 39 se puede observar la curva FAR vs FRR para el segundo experimento

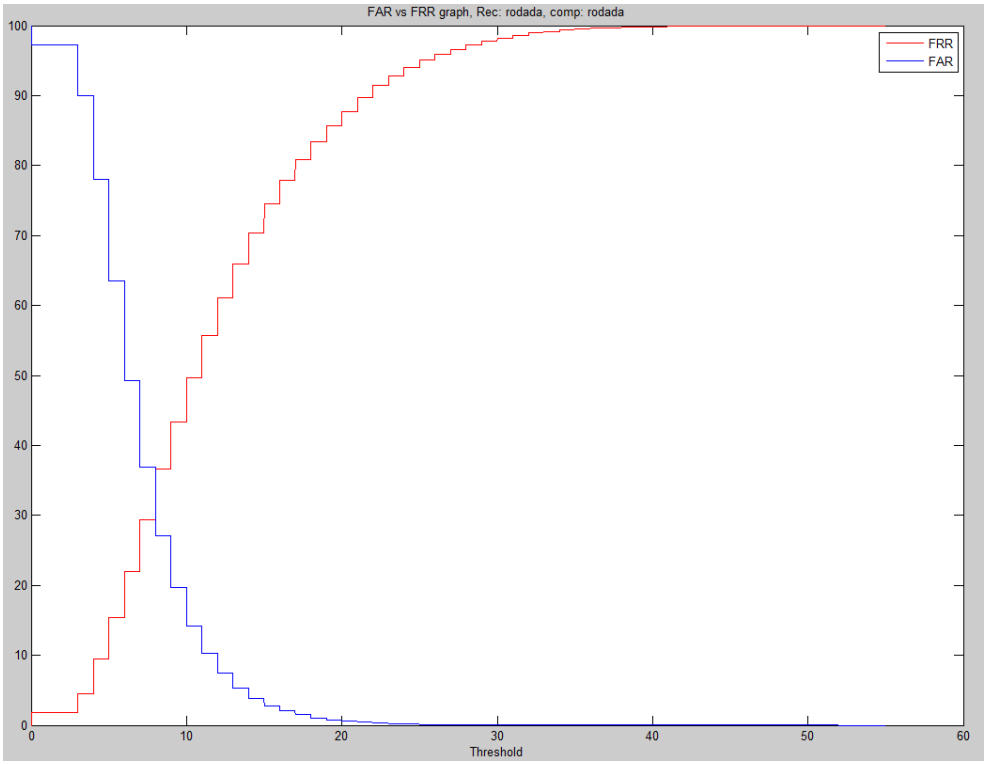


Figura 39 - Curva FARvsFRR para test 2, experimento 2

En este segundo experimento se ha realizado el reclutamiento con un sensor capacitivo y la verificación con un dispositivo óptico.

En este caso el EER tiene un valor de 38%. Este resultado es muy similar al del primer experimento, en el que se realiza el reclutamiento con el sensor óptico y la verificación con el sensor capacitivo, en el que el rendimiento era mucho menor que en los resultados del test 1 (en el que se realizaba tanto reclutamiento como verificación con el mismo sensor). Además, vemos que los errores aumentan si el reclutamiento se ha realizado con el sensor capacitivo y la verificación con el óptico que si se realizara al revés.

5.1.2.3. Resultados test 2

Se presentan ahora las curvas ROC y DET del primer test.

En la figura 40 se puede observar la curva ROC cuando el reclutamiento se ha realizado son un sensor óptico y la verificación con un sensor capacitivo (rojo) y cuando se ha realizado el reclutamiento con un sensor capacitivo y la verificación con un sensor óptico (azul).

La curva ROC con mayor rendimiento es aquella que corte más arriba en el eje de las ordenadas. En este caso podemos ver que la gráfica queda muy muy lejos de esta curva

ideal que se ha mencionado. En ambos experimentos la curva corta con el eje de ordenadas muy abajo, mostrando un rendimiento realmente bajo, como también muestran las gráficas FAR vs FRR.

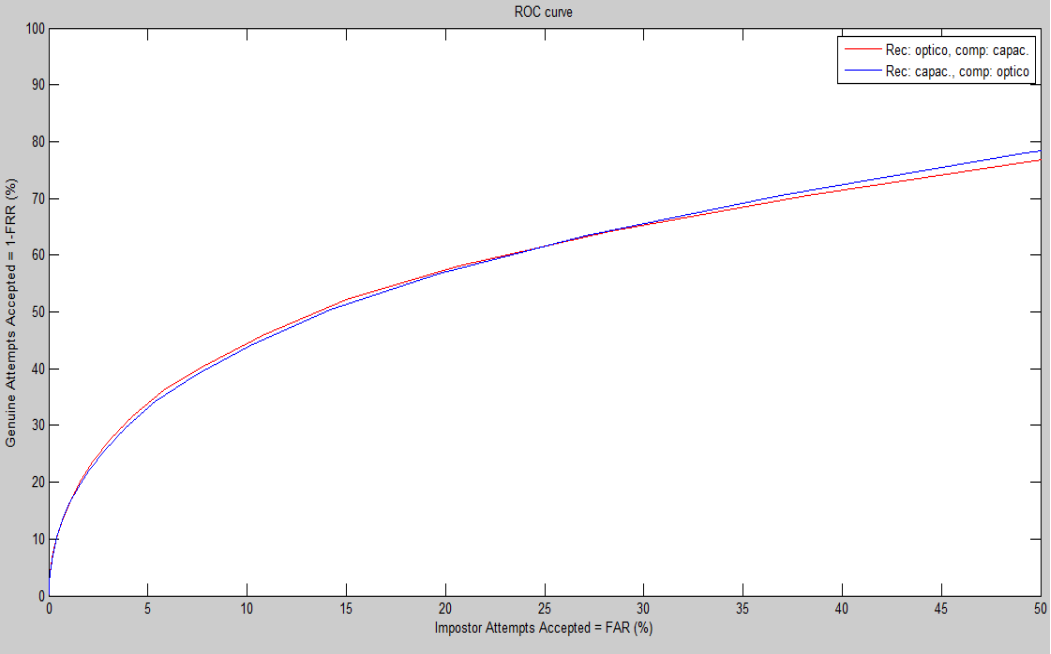


Figura 40 - Curva ROC para test 2

En la figura 41 se puede observar la curva DET para este test. La curva roja vuelve a ser para sensor capacitivo y la azul para el experimento óptico.

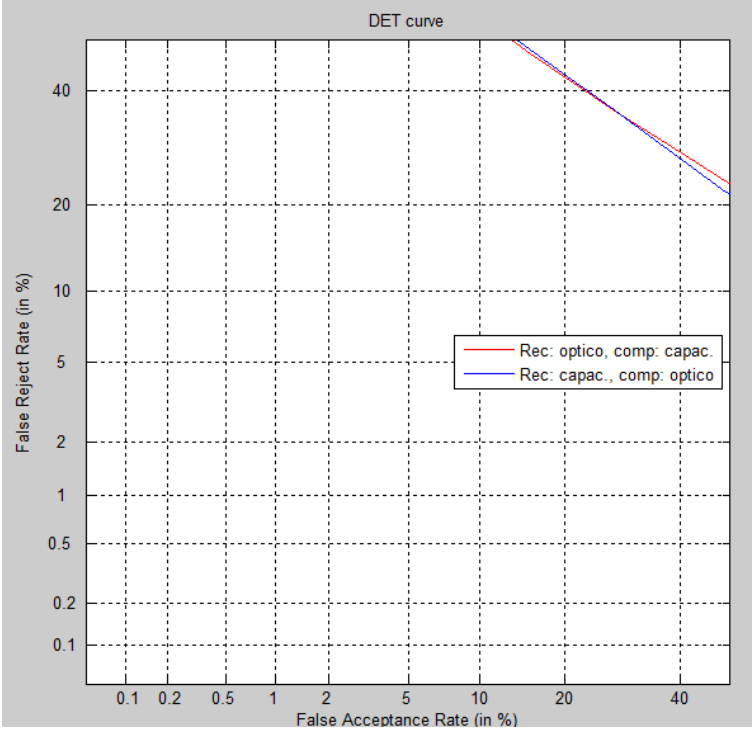


Figura 41 - Curva DET test 2

Se puede observar que la curva DET para ambos casos es prácticamente la misma, verificando así los valores de EER tan similares obtenidos anteriormente. Además se aleja mucho de la curva ideal, aquella que se acerca lo más posible al 0% en ambos ejes. Esto indica un rendimiento muy bajo.

5.1.2.4. Conclusiones test 2

Puede concluirse de este test que el rendimiento empeora mucho cuando se realiza el reclutamiento y la verificación con sensores de distinta tecnología. Además, se recibe el mismo resultado si se realiza en un sentido o en el otro. Es decir, reclutamiento con óptico y verificación con capacitivo o viceversa. En ambos casos el rendimiento cae mucho.

5.1.3. Comparación entre test

En la tabla 9 pueden observarse los distintos EER obtenidos para cada uno de los distintos experimentos. Se puede ver claramente que el EER aumenta de manera muy notable cuando se realizan los experimentos variando la tecnología con las que se hizo el reclutamiento y con la que se hizo el sensor. Por ello entre estos dos sensores la interoperabilidad es muy baja.

Tabla 9 - Comparación entre test

	Test 1		Test2	
	Experimento 1	Experimento 2	Experimento1	Experimento 2
Reclutamiento	Óptico	Capacitivo	Óptico	Capacitivo
Verificación	Óptico	Capacitivo	Capacitivo	Óptico
EER (%)	9	13	36	38

5.2. Análisis de usabilidad

Como se ha explicado anteriormente, el análisis de usabilidad sirve para saber de qué modo afecta al rendimiento la manera en la que los usuarios utilizan los distintos dispositivos de huella dactilar. La usabilidad representa la facilidad con la que los usuarios interactúan con el sistema. Por ello, a mejor usabilidad, menos errores serán cometidos y mayor rendimiento tendrá el sensor en cuestión.

En este análisis se analizarán todos los sensores ya que las gráficas los permiten hacer con gran facilidad. Aun así se concretará en cada parámetro las diferencias entre los dos sensores que se han utilizado para el análisis de interoperabilidad, el óptico 1 y el capacitivo.

Para este análisis, se ha creado la aplicación de MATLAB que se ha detallado en el capítulo 4. En ella se pueden elegir los parámetros que se deseen estudiar. Para la investigación se han elegido tres grupos en los que dividir a los usuarios. Estos parámetros han sido elegidos por ser los que pueden dar información más relevante y más interesante para al estudio. Se dividen en el estudio de la edad, la lateralidad y el sexo de los usuarios.

Además, ya que las muestras varían su tamaño dependiendo del grupo, se adjunta una tabla en la que se obtiene la cantidad de errores de cada tipo por usuario. De este modo resulta más fácil analizar los datos y comparar los distintos segmentos entre sí. Por ejemplo, al haber tres veces más hombres que mujeres, no tiene sentido comparar el número de errores de los dos géneros. Por ello, estas tablas tienen en cuenta el número de usuarios de cada segmento y proporciona un valor con el que poder comparar entre ellos, de modo que una comparación tenga sentido y se puedan obtener información estadísticamente correcta de ella.

Se intentará además encontrar la razón por la cual la frecuencia de los errores es distinta según el sensor, por ello se ha explicado el funcionamiento de los sensores en el apartado 3.2.2.

5.2.1. Edad

La edad es un buen modo de dividir a los usuarios que proporcionaron sus muestras. Esto es debido a que a mayor edad, normalmente se tiene menos costumbre de utilizar

tecnología y más errores es posible que se cometan. Se ha considerado que estos tres grupos de edad son los adecuados:

- menores de 30 años.
- entre 30 y 50 años.
- mayores de 50.

Se han elegido estas distribuciones ya que hasta los 30 años se puede considerar al individuo como 'nativo digital', aquellos que han nacido en la era tecnológica y no tienen problema al interactuar con ella. Los otros dos grupos se han elegido para tener un punto intermedio entre los 30 años y la edad máxima de los usuarios que dieron sus huellas, cerca de los 70.

5.2.1.1. Menores de 30

Se muestran a continuación los histogramas obtenidos de la aplicación diseñada, segmentando según la edad de los usuarios y según el error a estudiar.

FTD

Podemos ver en la figura 42 como el error FTD está claramente más presente en el señor de huella rodada. Dado el modo de utilización explicado en el apartado 3.2.2, en el que resultaba complicado rodar el dedo a la velocidad y ángulo correcto, es entendible que las muestras en muchas ocasiones no llegaran a detectarse dada la complejidad que requería el dar una muestra.

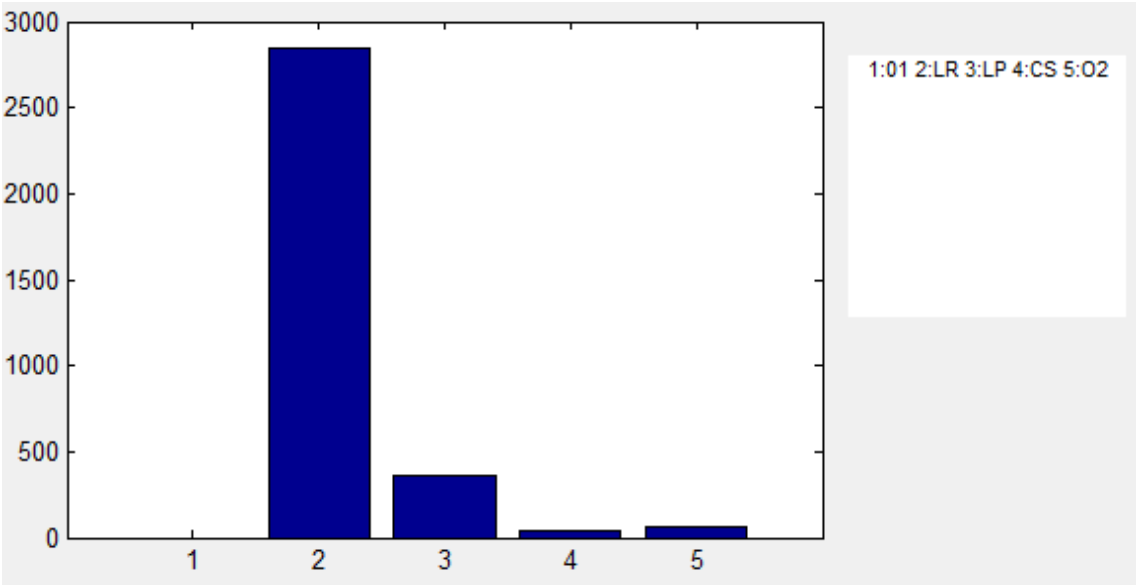


Figura 42 - Histograma FTD menores de 30

FTX

Podemos ver en la figura 43 como el error FTX está claramente más presente en el señor capacitivo. Esto viene dado por el pequeño área de captura con el que contaba este sensor. Es capaz de detectar la muestra por lo que no se produce un FTD con tanta frecuencia pero la muestra que es capturada no tiene calidad suficiente.

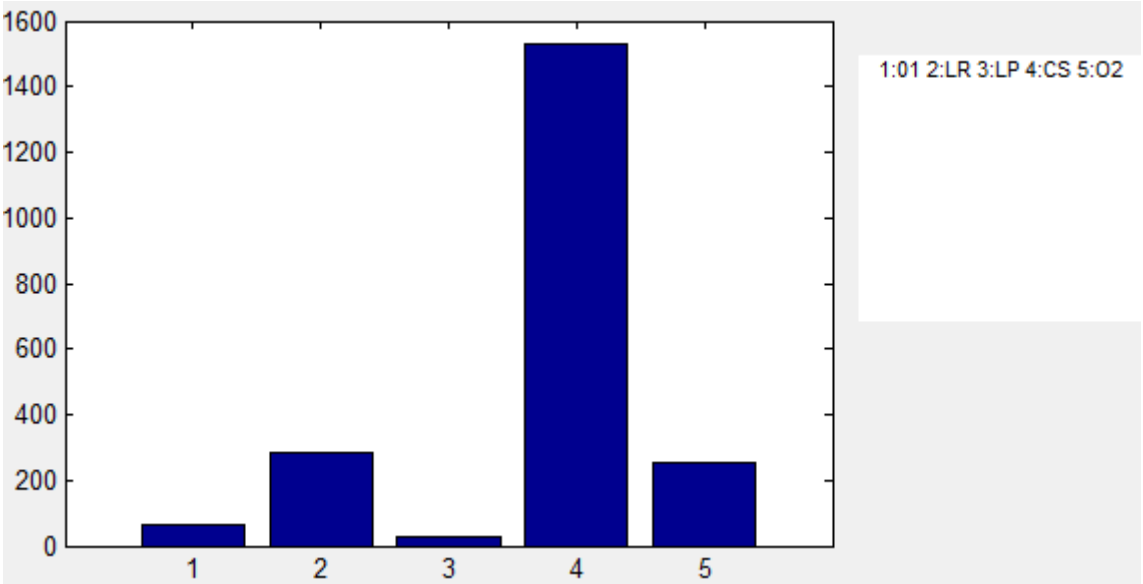


Figura 43 - Histograma FTX menores de 30

SPS

El SPS tiene lugar cuando se ha realizado una captura adecuada de la muestra. Es el evento que más sucedía. Puede parecer que el sensor de huella posada tiene un menor número de SPS pero, como se ha comentado en el apartado 3.2.2, sólo se tomaban una muestra por mano, resultando en tres veces menos muestras que los otros sensores, por lo que el número de huellas correctamente capturadas también es menor, de ahí que la barra en todos los errores SPS para el sensor de huella posada sea mucho menor.

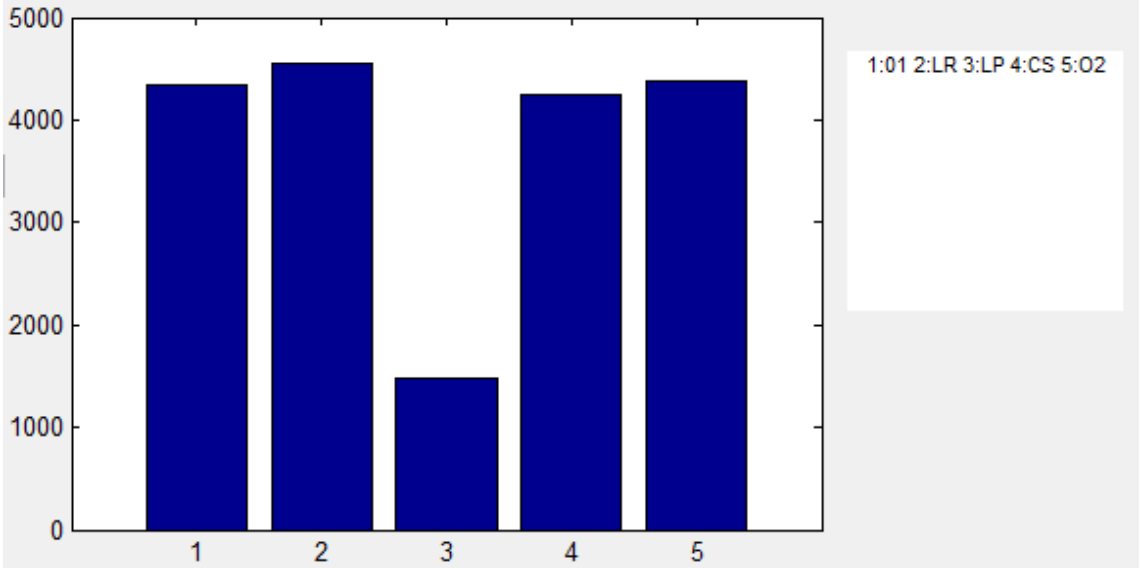


Figura 44 - Histograma SPS menores de 30

CI

Este error vuelve a estar más presente en el sensor capacitivo. Dado a su reducido tamaño resultaba más intuitivo utilizarlo para el dedo pulgar de ambas manos por lo que en ocasiones se repetía este dedo cuando se debía presentar otro dedo, dando lugar al error CI.

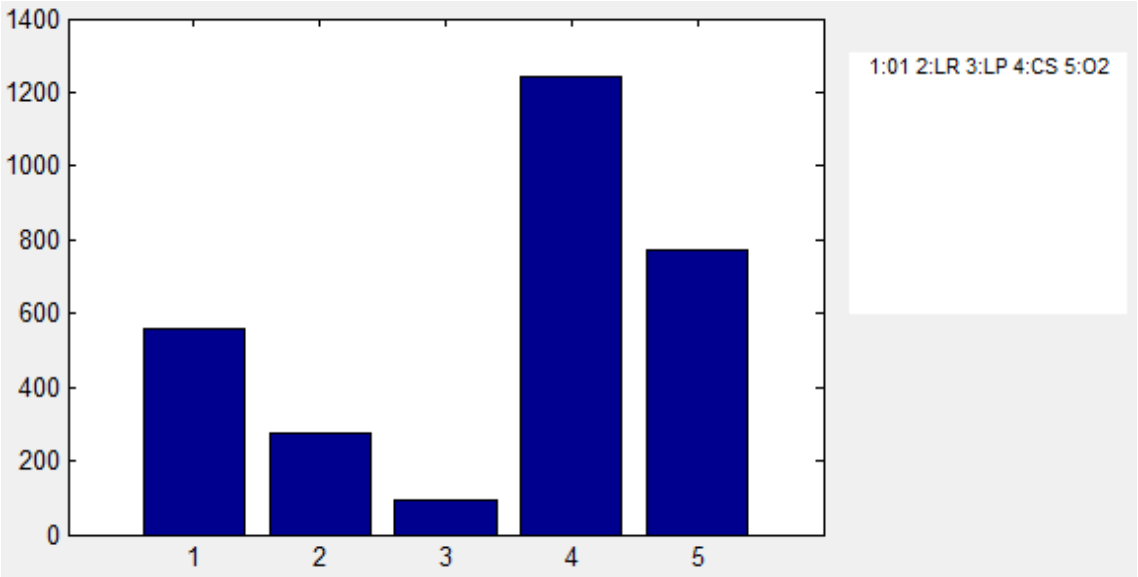


Figura 45 - Histograma CI menores de 30

Observando la tabla 10 se puede ver que la diferencia de aparición de los distintos tipos de error es muy marcada, aun así el número de muestras capturadas con éxito es superior a los errores realizados.

Tabla 10 – Errores por persona según sensor en menores de 30

Error\Sensor	O1	LR	LP	CS	O2
FTD	0	55,6	7	0,72	1,3
FTX	1,24	5,68	0,5	29,42	5,12
SPS	85,24	89,18	28,9	84	86
CI	11	5,5	1,8	24,4	15

5.2.1.2. Entre 30 y 50

El segundo rango de edad sigue la misma tónica que el anterior, repitiéndose la frecuencia de aparición de errores según el sensor. Cabe destacar que hay varios errores que no ocurrieron en ciertos sensores.

FTD

Este error sigue estando mucho más presente en el sensor de huella rodada.

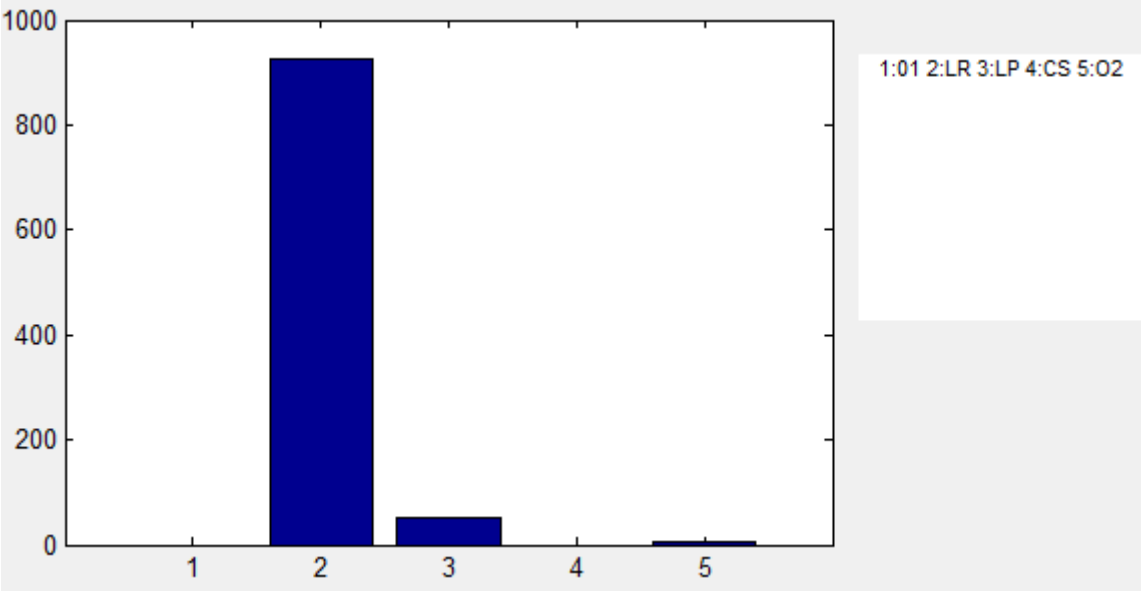


Figura 46 - Histograma FTD entre 30 y 50

FTX

Volvemos a ver la mayor frecuencia de este error en el sensor capacitivo.

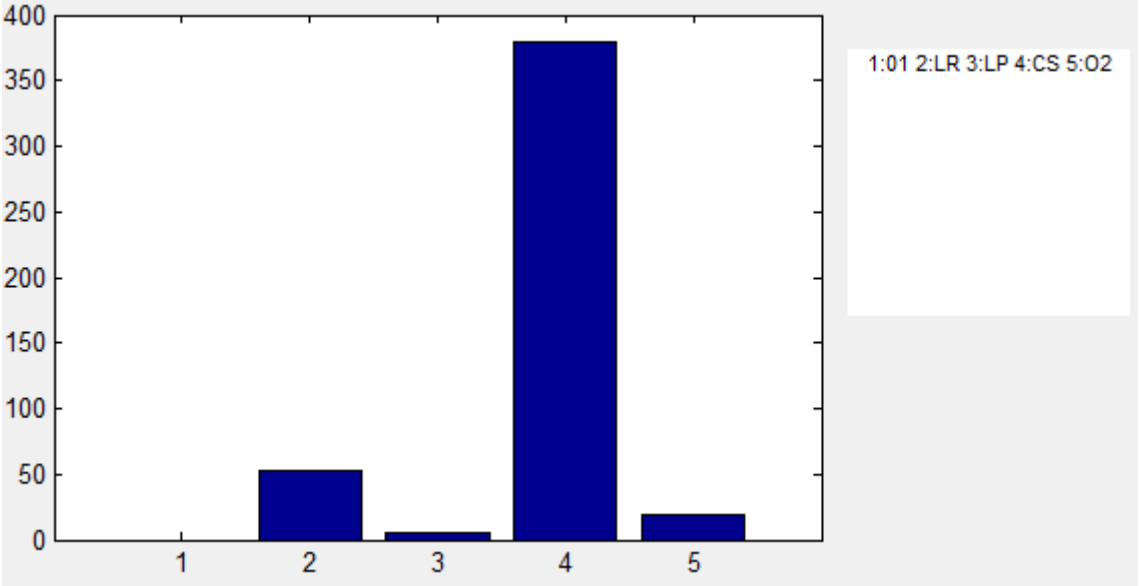


Figura 47 - Histograma FTX entre 30 y 50

SPS

La única diferencia en la aparición del suceso SPS, es que es ligeramente inferior a los de los usuarios menores de 30 años. Esto se debe a la mayor facilidad de la gente joven a interactuar con estos dispositivos.

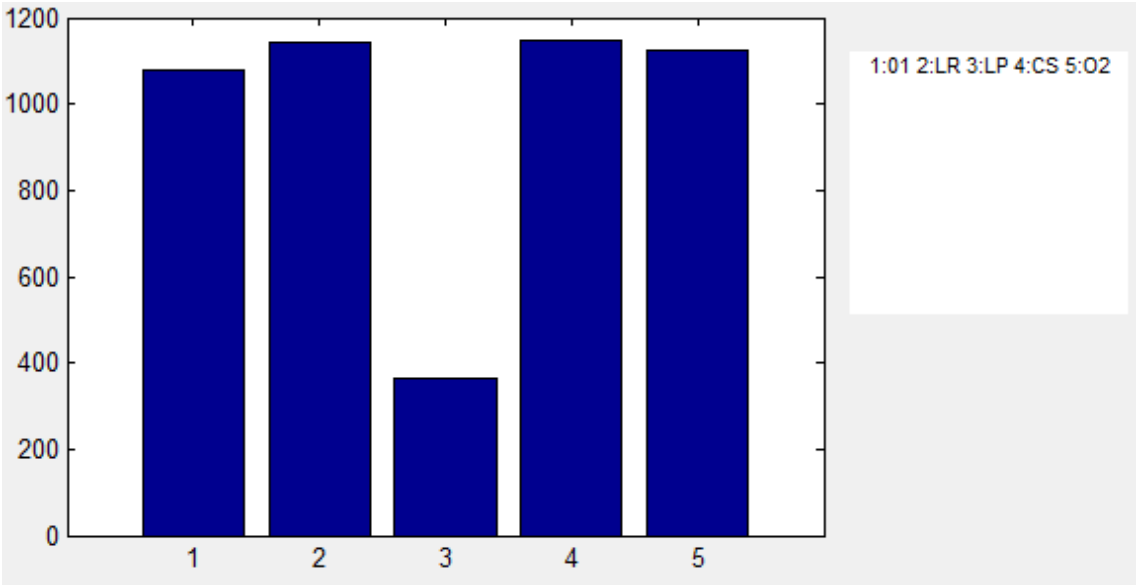


Figura 48 - Histograma SPS entre 30 y 50

CI

En este caso ocurre al contrario que con los SPS, como era de esperar. En esta franja de edad se incrementa ligeramente la aparición de errores.

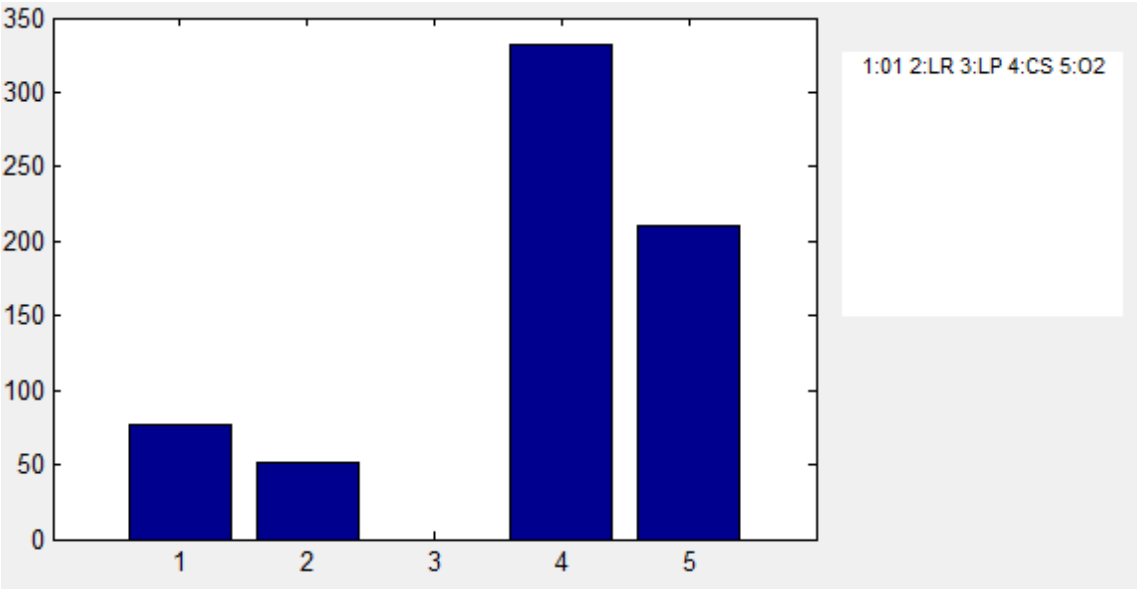


Figura 49 - Histograma CI entre 30 y 50

Tabla 11 - Errores por persona según sensor entre 30 y 50

Error\Sensor	O1	LR	LP	CS	O2
FTD	0	62,2	4	0	0,3
FTX	0	3,3	0,3	23,7	1,6
SPS	72,75	103,8	24,5	75	74,9
CI	5,1	3,2	0	21,25	14,4

5.2.1.3. Mayores de 50

Lo más característico de este grupo de edad es el aumento en el número de errores por persona. Aún así los tipos de error se mantienen con el mismo ratio, al igual que en los dos casos anteriores.

FTD

Vuelve a incrementarse la aparición de este error debido a la falta de costumbre de uso de los dispositivos.

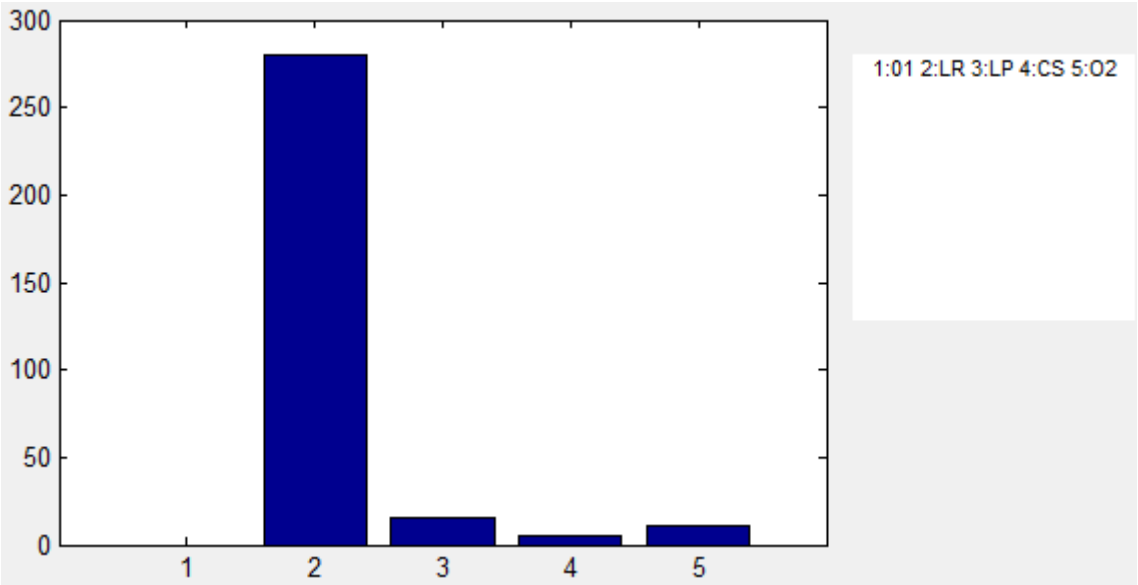


Figura 50 - Histograma FTD mayores de 50

FTX

Caso análogo al del error FTD.

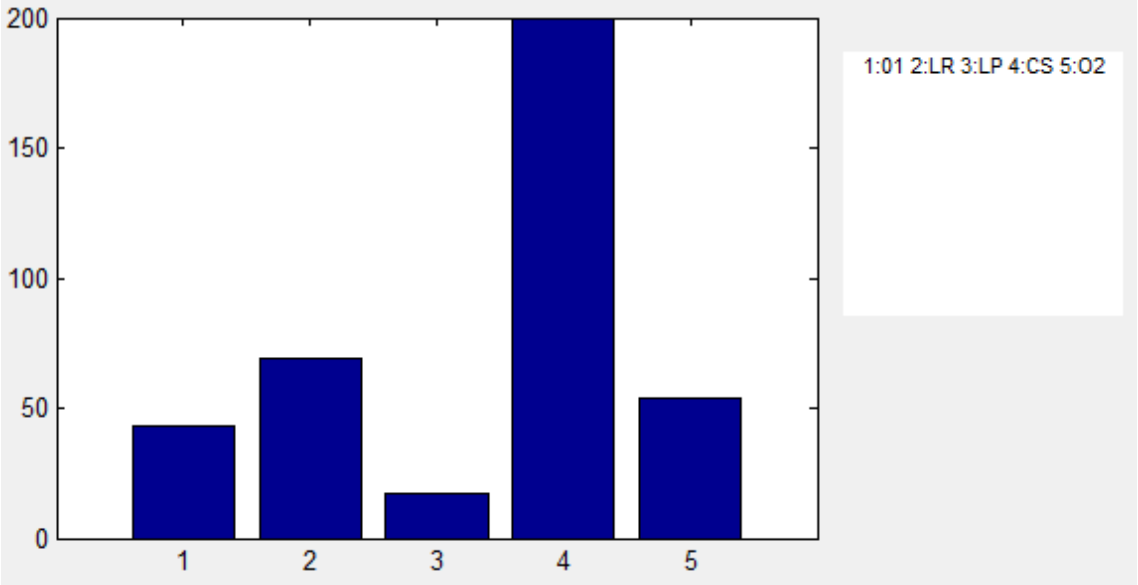


Figura 51 - Histograma FTX mayores 50

SPS

Cabe destacar la dificultad que se encentra a la hora de procesar correctamente la huella para el sensor de huella rodada. Esto vuelve a marcar las dificultades que se encuentran

con este sensor debido a su difícil utilización y más aún si la edad es más avanzada ya que no se cuenta con la misma agilidad ni la misma flexibilidad en las manos para poder utilizar este sensor de manera adecuada.

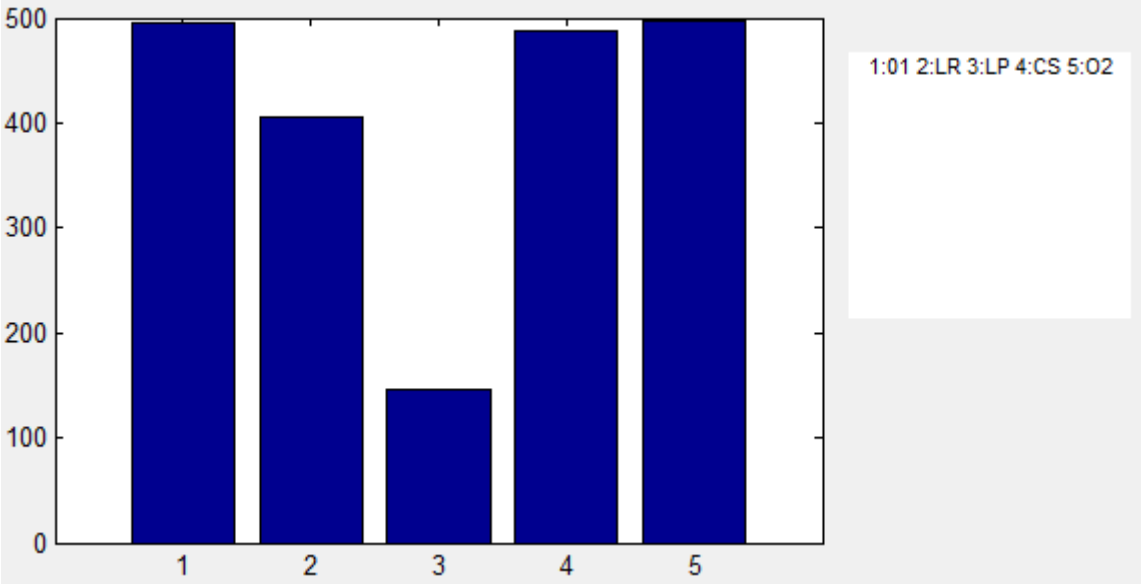


Figura 52 - Histograma SPS mayores 50

CI

Vuelve a repetirse el incremento de errores de este tipo, destacando por su incremento en el sensor óptico 1. En este caso puede deberse a la aleatoriedad que se ha comentado en el apartado 3.2.1.1.2, que hacía más complicado realizar un buen uso del sistema.

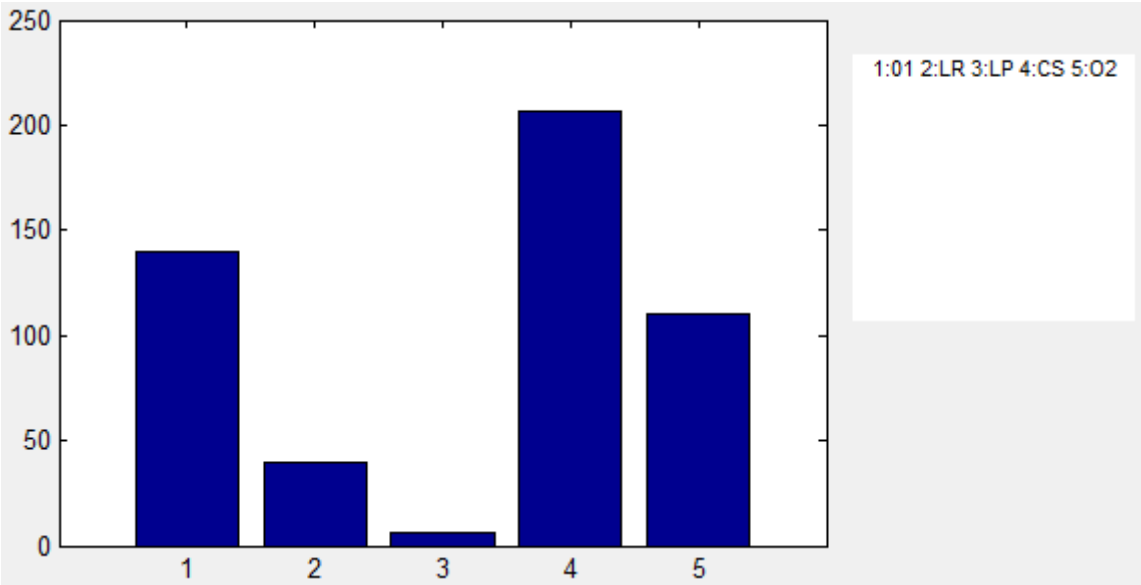


Figura 53 - Histograma CI mayores 50

Tabla 12 - Errores por persona según sensor en mayores de 50

Error\Sensor	O1	LR	LP	CS	O2
FTD	0	46,6	2,5	0,83	1,8
FTX	7,1	11,5	2,8	33,3	9
SPS	82,5	67,5	24,3	81,1	82,8
CI	23,3	6,6	2,5	34,5	18,3

5.2.1.4. Conclusiones según edad

Se puede observar una estrecha relación entre los grupos de menores de 30 años y el grupo entre 30 y 50.

En los dos grupos se cometieron el mayor número de errores en el sensor de huella rodada, seguido del capacitivo, el óptico 2, el óptico 1 y por último, a mucha distancia, el sensor de huella posada.

Además en ambos grupos se repite la frecuencia con las que se cometen los distintos tipos de errores, siendo el más frecuente el FTD, el CI y por último el FTX. Esto muestra que la presentación de las huellas para estos dos grupos no fue el principal problema.

En cuanto al grupo de mayores de 50, comparte el número de errores total y el orden en que ocurrieron según los sensores. A la hora de analizar los tipos de errores que se cometieron sí que se encuentran ciertas diferencias. El orden decreciente de errores cometidos fue: CI, FTX y el FTD. Existe una gran diferencia entre los errores CI con respecto a los otros dos grupos, indicando con ello que el grupo de mayores de 50 años tuvieron mayores problemas a la hora de interactuar con los sensores provocando un mayor número de errores de este tipo. Además a lo largo de la vida , aunque la huella no se modifica, sí que sufre deterioro debido al uso de las manos. Es por ello que las personas mayores también tengan problemas a la hora de conseguir que el sensor detecte sus huellas.

Enfocando este estudio de la edad a los dos sensores que más se tratan en este TFG, se puede observar que el sensor capacitivo resultó mucho más problemático a la hora de capturar las muestras. Concretamente causó muchos más errores en los errores FTX y CI. En cambio, el sensor óptico que se está estudiando, el O1, no causó tantos errores como el capacitivo. Es por ello que puede concluirse que la usabilidad es menor en el sensor capacitivo que en el sensor óptico 1, ocurre de mismo modo para todos los segmentos de edad.

5.2.2. Lateralidad

Se eligió estudiar la lateralidad ya que los sensores podrían acarrear problemas según cómo estuvieran diseñados físicamente. Gran parte de la sociedad es diestra mientras

que sólo un 10% es zurda [17]. Es por ello que los diseños suelen estar enfocados a personas diestras causando incomodidades de uso a las personas zurdas.

5.2.2.1. Diestros

El mayor número de errores se registró en el sensor de huella rodada y el sensor capacitivo, seguidos de los dos ópticos casi igualados y por último el de huella posada.

FTD

En el sensor de huella rodada se tuvieron muchos problemas a la hora de capturar las huellas por su complicada manera de obtener las muestras.

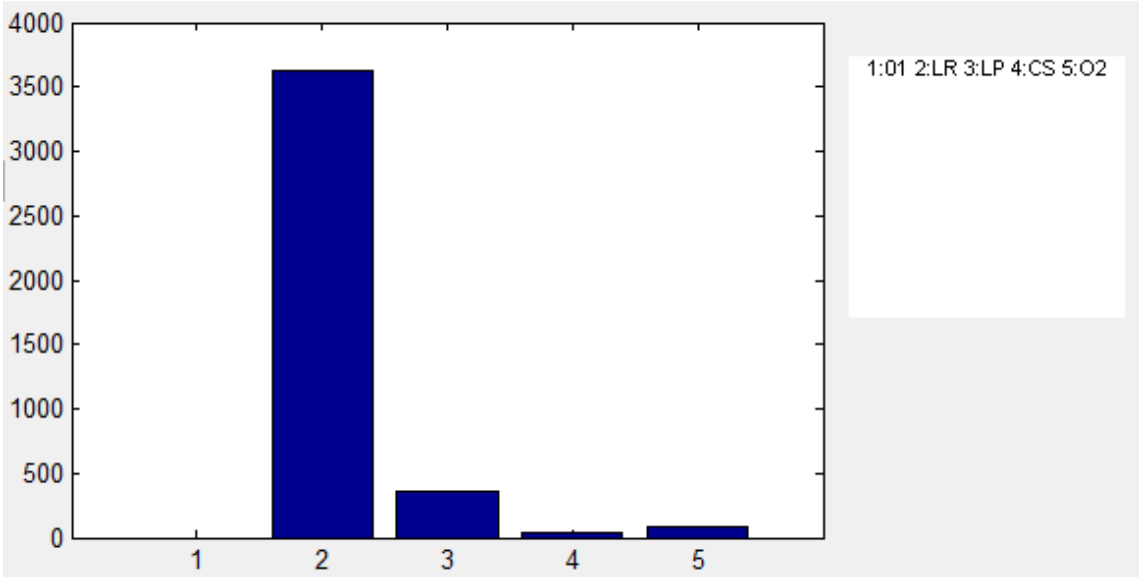


Figura 54 - Histograma FTD para diestros

FTX

Una vez obtenidas las muestras, se observa que el sensor de huella rodada ha adquirido con calidad las muestras mientras que el sensor capacitivo, que no generó apenas errores FTD, genera una gran cantidad de errores FTX. Esto quiere decir que la extracción de información de la huella posterior a la presentación no es buena. Se debe a que el sensor de huella rodada es muy complicado de utilizar pero de utilizarlo de manera correcta captura las huellas con una mejor calidad que el sensor capacitivo que es más intuitivo de utilizar pero genera unas muestras de mala calidad.

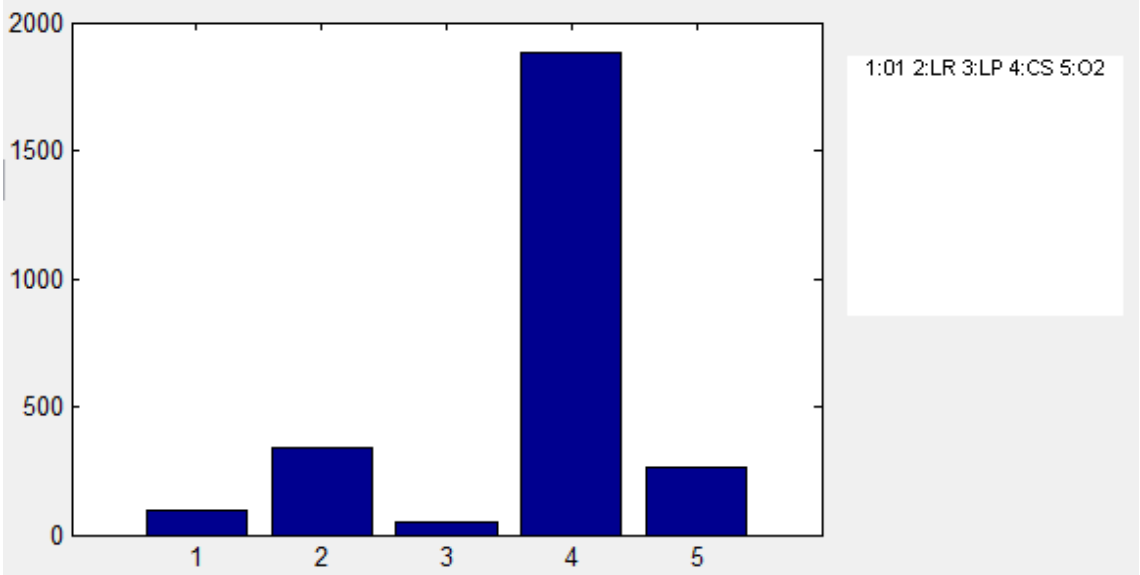


Figura 55 - Histograma FTX para diestros

SPS

No hay gran información que se pueda extraer de esta gráfica ya que todos los sensores obtuvieron resultados parecidos. Recuérdese que el SPS en la huella posada capta menos huellas por manos.

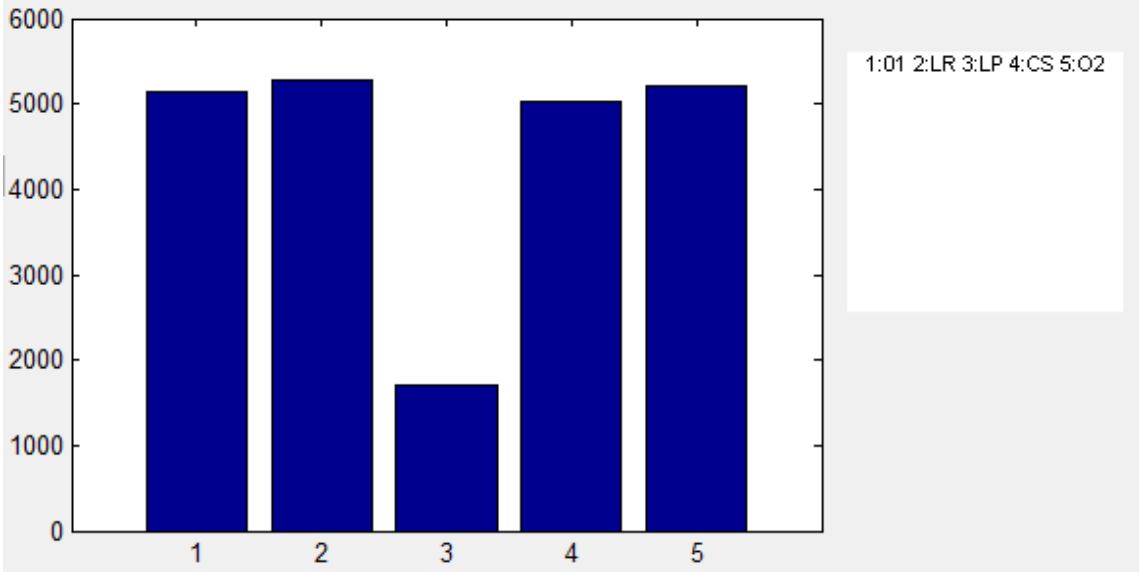


Figura 56 - Histograma SPS para diestros

CI

Vuelve a ser el sensor capacitivo el que más errores de tipo CI genera.

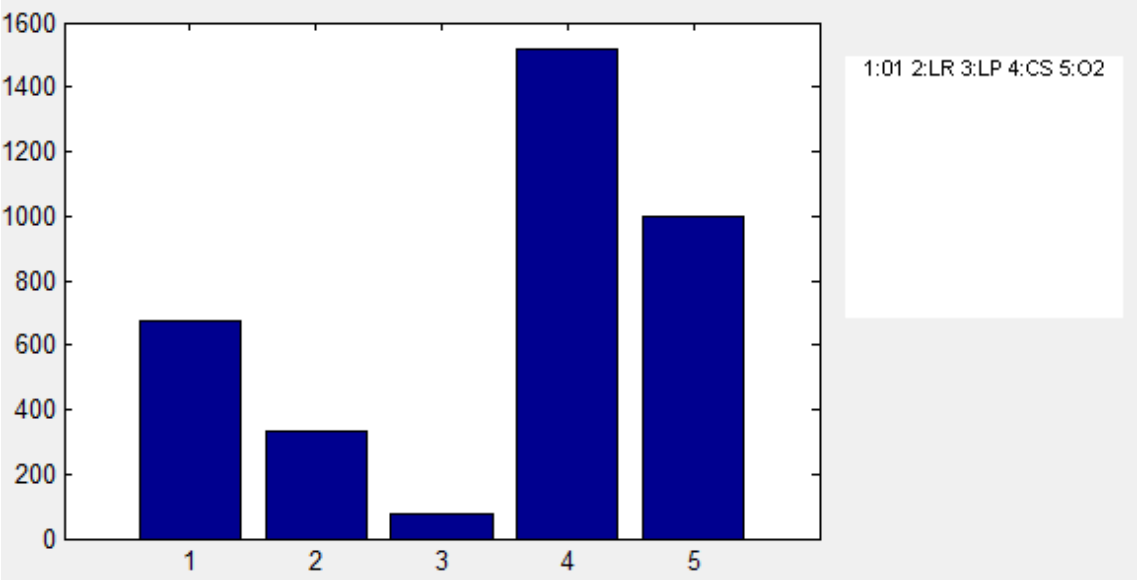


Figura 57 - Histograma CI para diestros

Tabla 13 - Errores por persona según sensor en diestros

Error\Sensor	O1	LR	LP	CS	O2
FTD	0,0	57,5	5,7	0,7	1,3
FTX	1,6	5,4	0,7	29,9	4,2
SPS	81,5	83,8	27,1	79,9	82,8
CI	10,7	5,3	1,2	24,0	15,8

5.2.2.2. Zurdos

Este grupo comparte con gran similitud los resultados obtenidos por el grupo de usuarios diestros.

FTD

Cabe destacar la inexistencia de errores de este tipo en tres de los sensores. Es posible que sea causado por la baja participación de voluntarios zurdos.

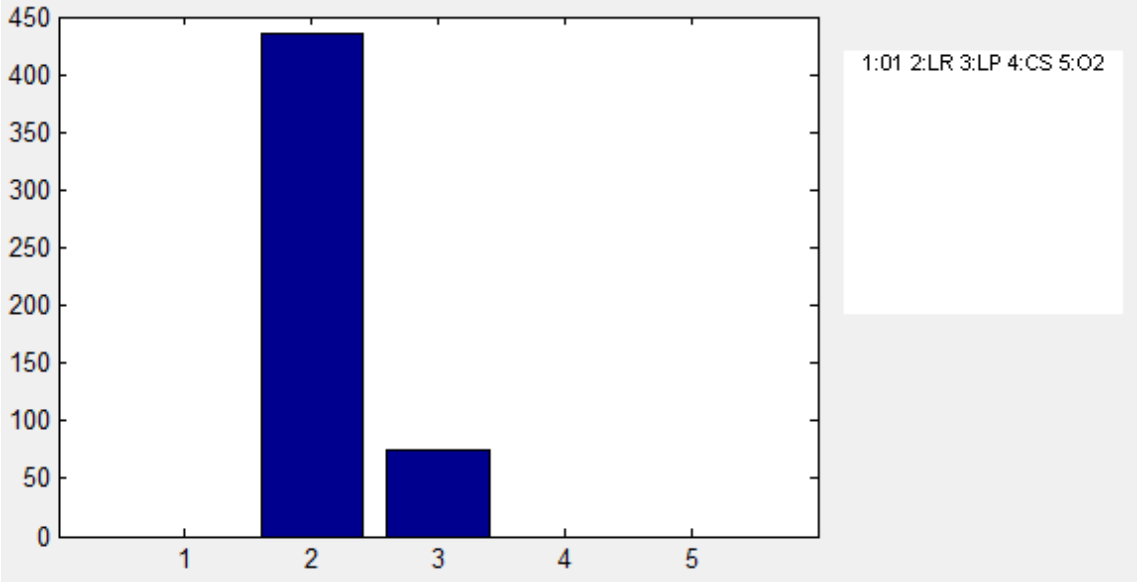


Figura 58 - Histograma FTD para zurdos

FTX

Caso análogo al de los usuarios diestros, sin diferencias apreciables.

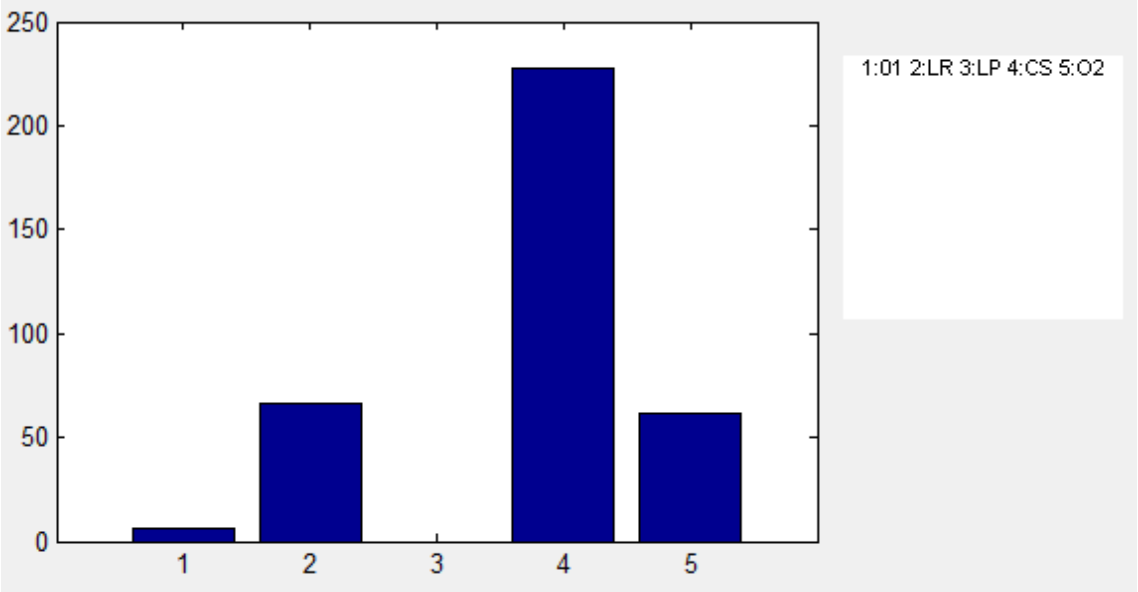


Figura 59 - Histograma FTX para zurdos

SPS

Puede apreciarse en los usuarios zurdos un mejor número de SPS que en el caso de los usuarios diestros.

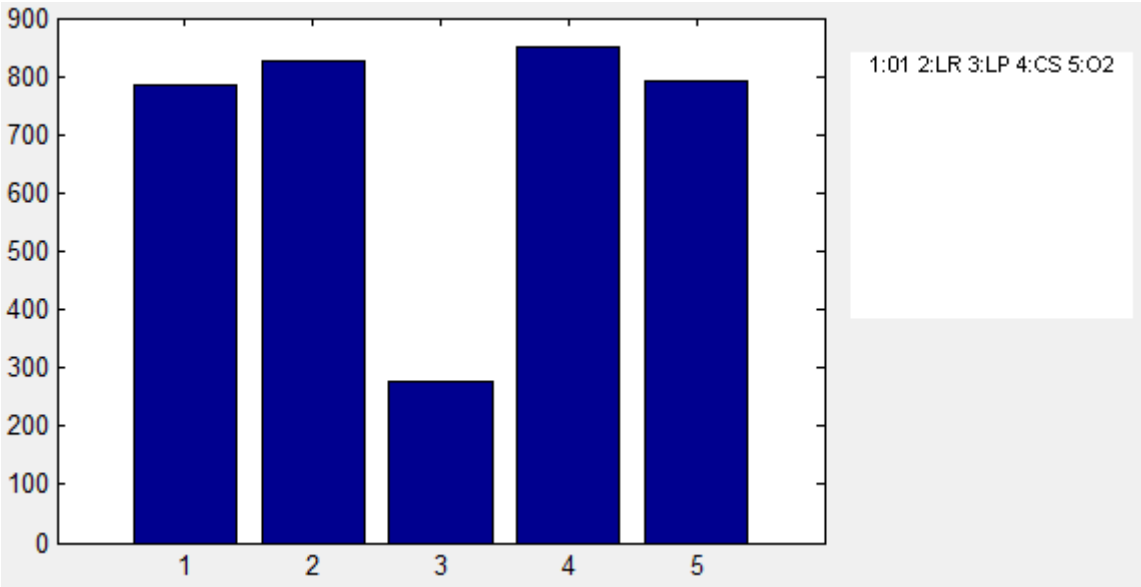


Figura 60 - Histograma SPS para zurdos

CI

Volvemos a tener un caso prácticamente igual que en el de los usuarios diestros en el que el sensor capacitivo genera mayor número de errores CI.

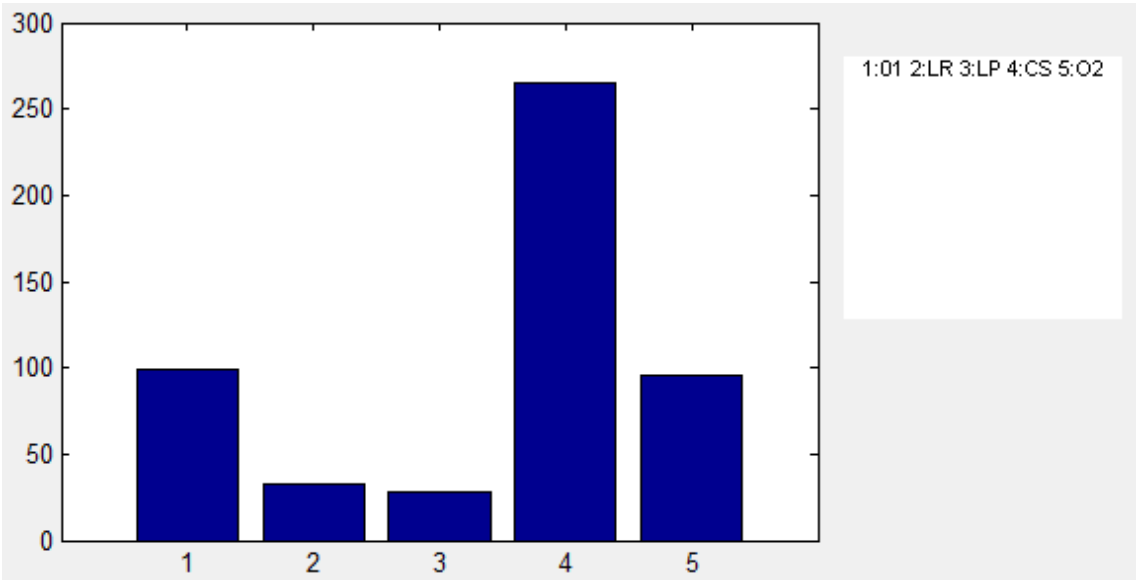


Figura 61 - Histograma CI para zurdos

Tabla 14 - Errores por persona según sensor en zurdos

Error\Sensor	O1	LR	LP	CS	O2
FTD	0,0	48,4	8,2	0,0	0,0
FTX	0,7	7,3	0,0	25,3	6,9
SPS	87,3	91,7	30,7	94,6	88,1
CI	11,0	3,7	3,1	29,4	10,7

5.2.2.3. Conclusiones según lateralidad

Ambos grupos comparten el hecho de que el mayor número de errores aparecieron en los sensores de huella rodada y en el capacitivo. Causado de nuevo por el difícil manejo del sensor de huella rodada y del pequeño espacio de captura del sensor capacitivo. Comparando los resultados entre ambas lateralidades se puede observar un patrón común. Tanto diestros como zurdos tuvieron un mayor número de errores FTD, seguido por errores CI y por último, FTX.

Es apreciable la diferencia de errores que aparecen entre el sensor óptico 1 y el capacitivo. Mientras que no sucedió ningún error de tipo de error FTD en ninguno de los dos, cuando se analizan los errores FTX y CI se puede apreciar un cambio muy significativo en la comparación. Se vuelve a mostrar, como se vio en el estudio de la usabilidad según la edad, que la usabilidad en los sensores capacitivos es menor para ambas lateralidades.

Se puede concluir que la lateralidad no influye en gran medida en estos sensores que se han estudiado ya que las presentaciones erróneas y correctas son casi iguales en ambos casos.

5.2.3. Sexo

El sexo es una característica muy diferenciadora entre seres humanos, es por ello que se decidió realizar el estudio para ver si existe alguna diferencia en cómo interactúan las personas de distinto sexo con los dispositivos de huellas dactilares.

5.2.3.1. Hombres

Los errores totales según sensor se diferencian claramente. En el que más errores se cometieron fue en el de huella rodada, seguido por el capacitivo.

FTD

Vuelve a ocurrir que la dificultad de uso del sensor de huella rodada causó un gran número de errores en los que el sensor no era capaz de detectar la huella.

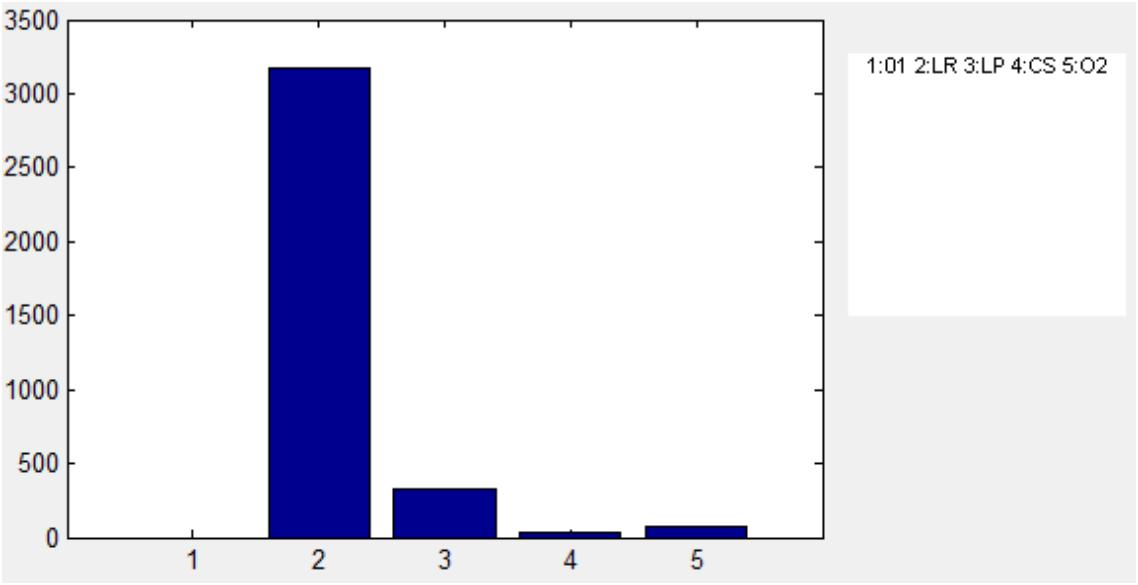


Figura 62 - Histograma FTD para hombres

FTX

Vuelve a suceder que la mayor frecuencia de FTX ocurre en el sensor capacitivo debido a la mala calidad que obtiene de las muestras que se le presentan.

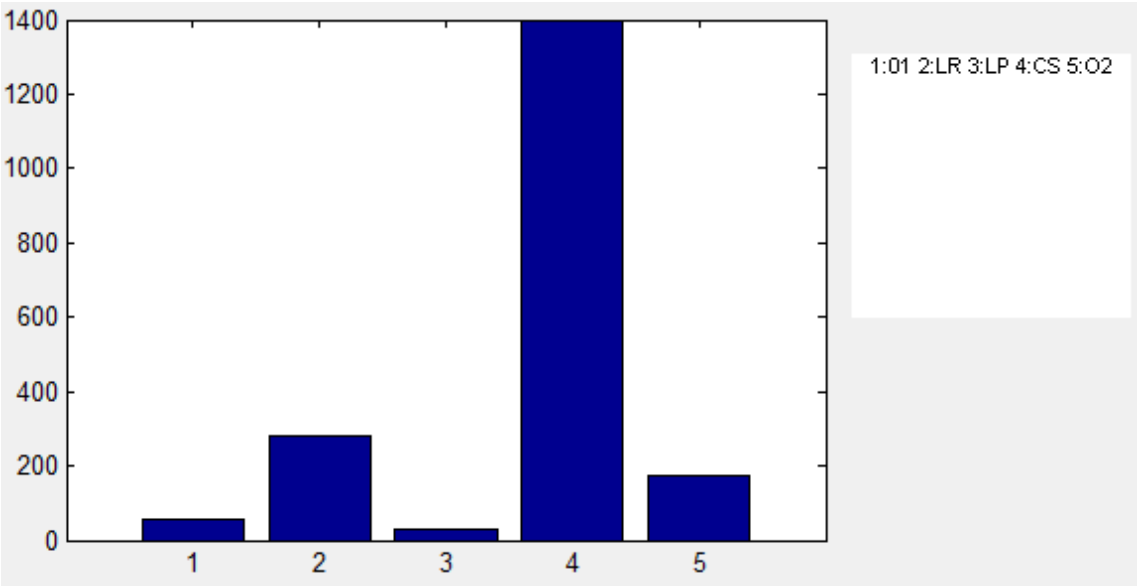


Figura 63 - Histograma FTX para hombres

SPS

Como a lo largo de todo el proyecto, se sigue teniendo un número muy elevado de SPS, siendo prácticamente igual en todos los sensores.

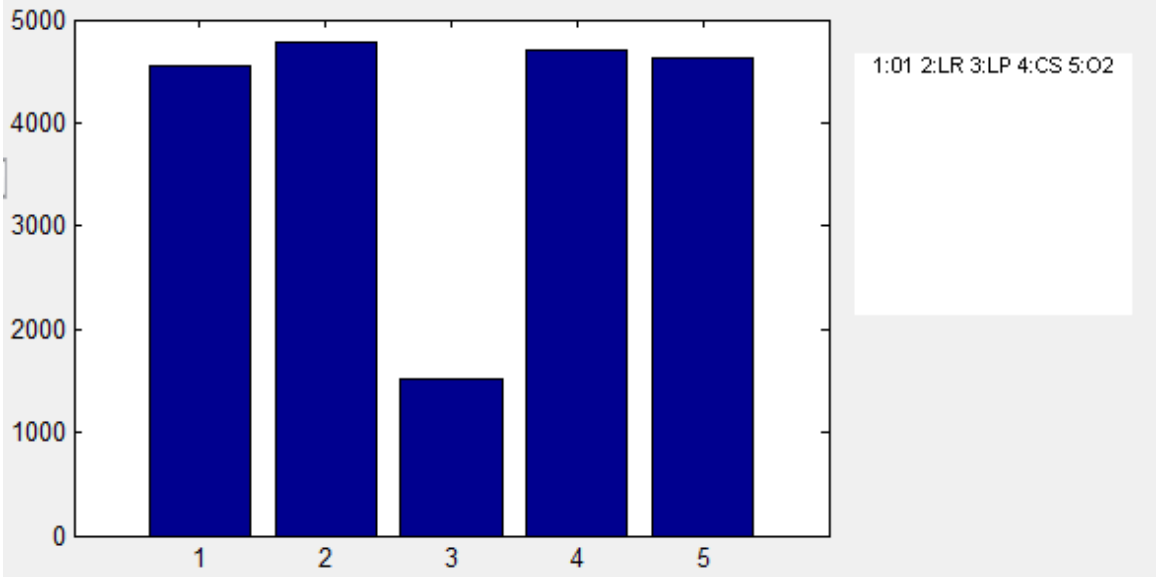


Figura 64 - Histograma SPS para hombres

CI

Puede observarse que de nuevo el sensor capacitivo ha sido el que más errores de tipo CI ha generado debido a las razones argumentadas a lo largo de este apartado 5.2.

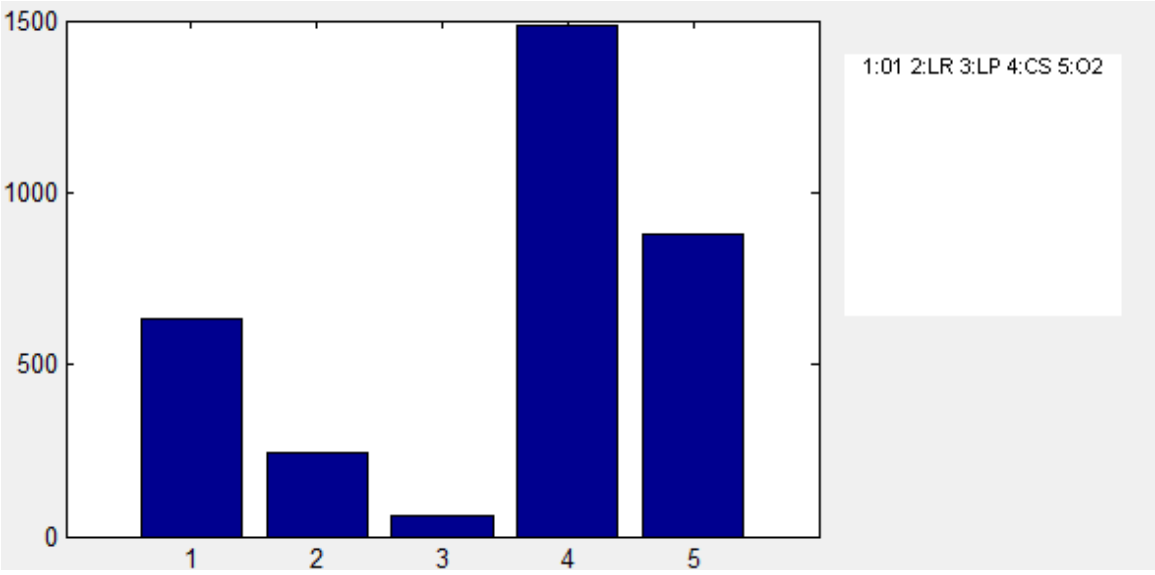


Figura 65 - Histograma CI para hombres

Tabla 15 - Errores por persona según sensor en hombres

Error\Sensor	O1	LR	LP	CS	O2
FTD	0,0	57,7	5,9	0,7	1,4
FTX	1,0	5,1	0,6	25,4	3,2
SPS	82,9	87,0	27,7	85,4	84,1
CI	11,5	4,4	1,1	27,1	16,0

5.2.3.2. Mujeres

Los errores totales según sensor se parecen claramente a los de los hombres. En el que más errores se cometieron fue en el de huella rodada, seguido por el capacitivo, como viene ocurriendo durante todo el TFG.

FTD

Refleja prácticamente el mismo resultado que los hombres.

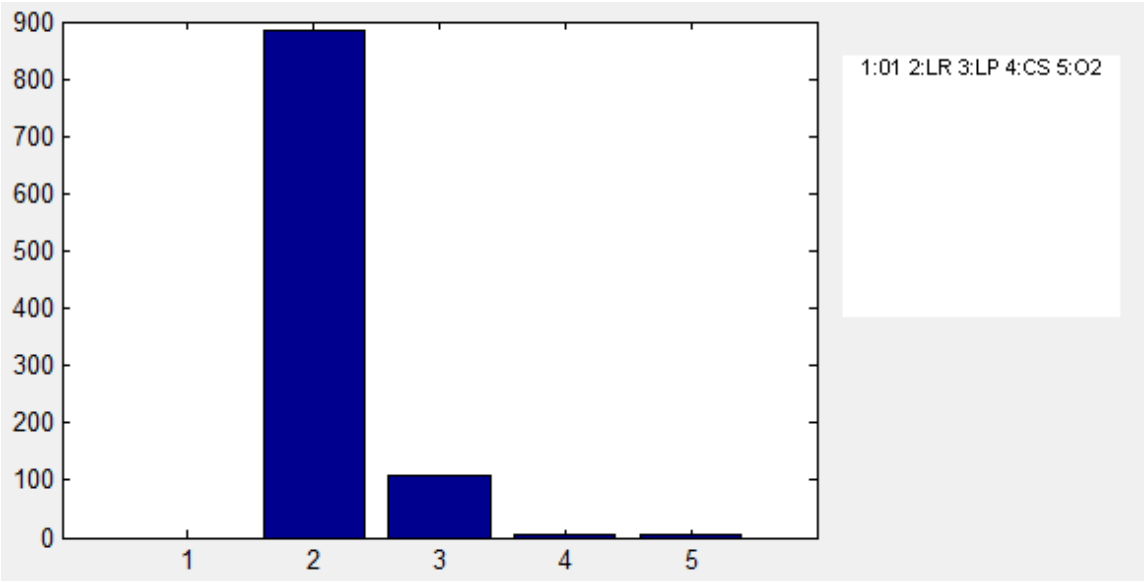


Figura 66 - Histograma FTD para mujeres

FTX

Aquí se cometió de manera conjunta, mayor número de errores FTX, por lo que las muestras que proporcionaban las mujeres resultaban de menor calidad, puede deberse al uso de cosméticos y cremas de manos.

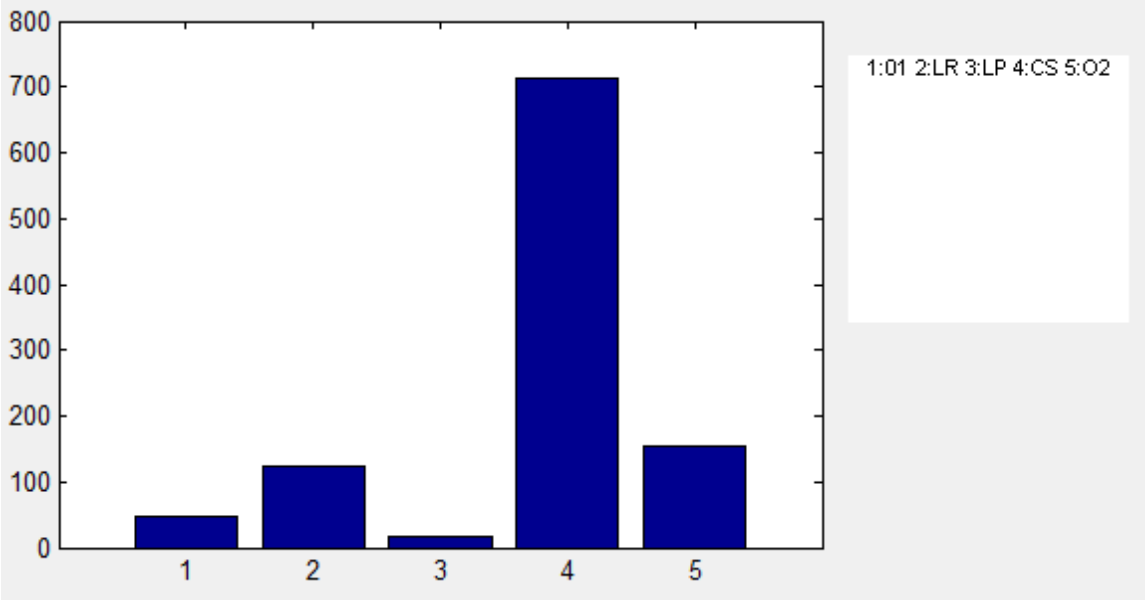


Figura 67 - Histograma FTX para mujeres

SPS

En cuanto a los SPS no se aprecian diferencias con los hombres.

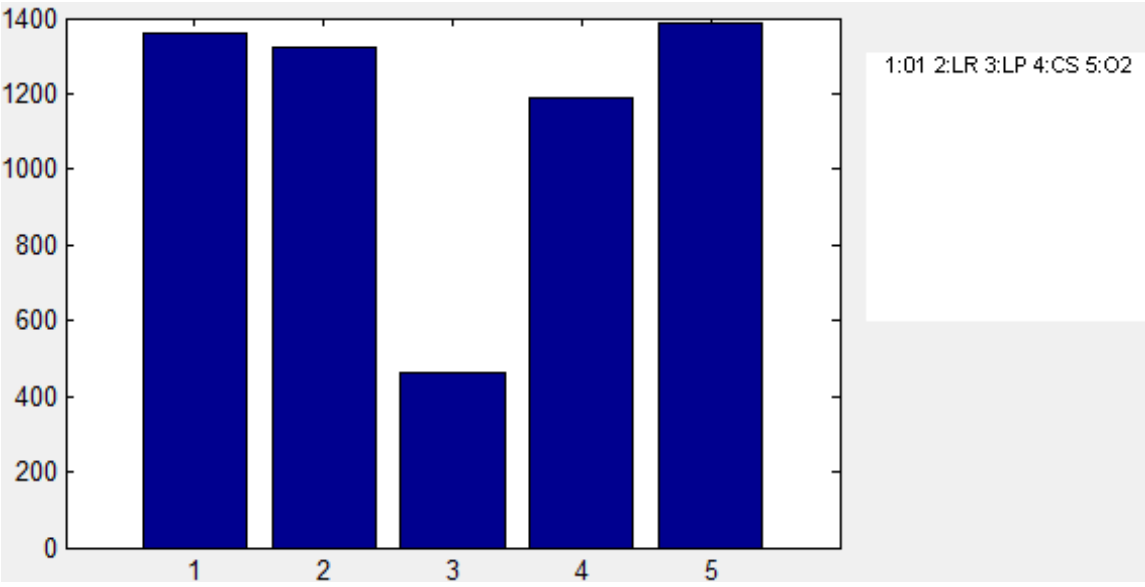


Figura 68 - Histograma SPS para mujeres

CI

Volvemos a encontrar diferencias en los errores CI, la mujer cometió menos errores de este tipo por lo que la interacción con los sensores es mejor en el sexo femenino que en el masculino.

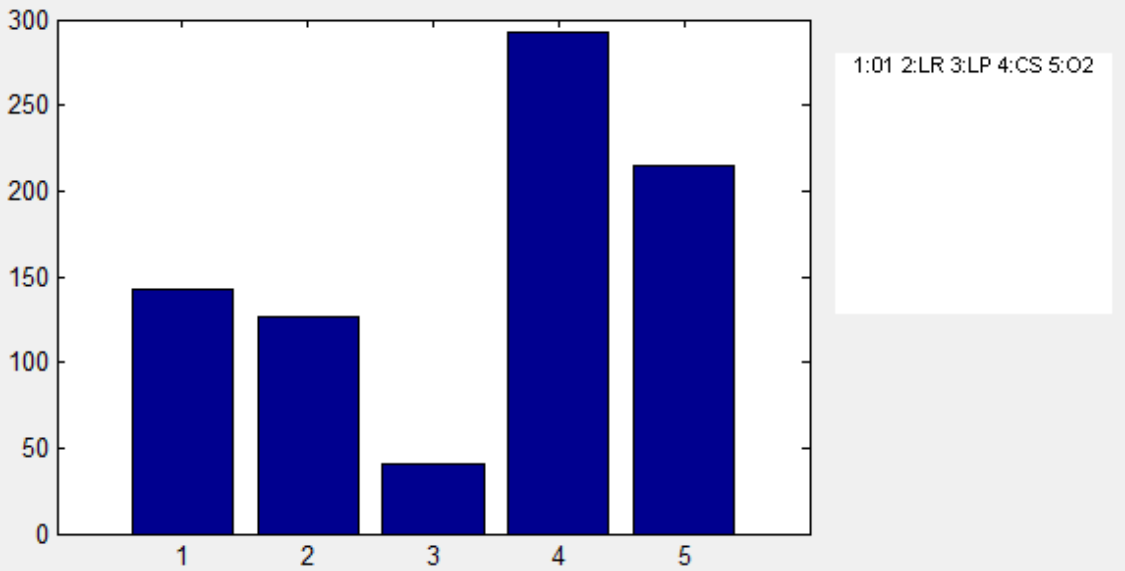


Figura 69 - Histograma CI para mujeres

Tabla 16 - Errores por persona según sensor en mujeres

Error\Sensor	O1	LR	LP	CS	O2
FTD	0,0	51,9	6,3	0,3	0,3
FTX	2,8	7,2	0,9	41,9	9,1
SPS	80,1	77,8	27,3	70,1	81,6
CI	8,4	7,5	2,4	17,2	12,6

5.2.3.3. Conclusiones según sexo

Entre ambos sexos apenas hay diferencias en cuanto a los errores que se cometen dependiendo del sensor. El sensor en el que más errores se cometieron fue el de huella rodada, seguido por el capacitivo.

Donde sí se encuentran diferencias es en qué errores se cometieron. Mientas que en los hombres el error que menos se cometió fue el FTX, en las mujeres fue el CI. Esto indica que las mujeres interactuaron mejor con los sensores ya que fueron capaces de realizar mayor número de presentaciones correctas.

Se repite de nuevo la comparación, que ha ocurrido en los grupos de edad y lateralidad, entre el sensor capacitivo y el sensor óptico 1. Mientras que el óptico 1 goza de una usabilidad bastante buena en ambos sexos, el capacitivo genera una cantidad de errores mucho mayor en los tipos FTX y CI.

6. Conclusiones y líneas futuras

6.1. Conclusiones

De este TFG se han podido obtener algunas conclusiones de la interoperabilidad y de la usabilidad.

A partir de una BBDD, se han realizado dos tipos de análisis, de interoperabilidad y de usabilidad.

El análisis de interoperabilidad se realizó con una aplicación existente de la que se obtuvieron las tasas de rendimiento de dos tecnologías distintas. Se intercambió la manera en la que se combinan los sensores para poder comparar como varía de hacer el reclutamiento y la verificación con la misma tecnología o con tecnologías distintas.

De este análisis, y observando los resultados, se puede concluir que el rendimiento es mucho mayor cuando se realiza el sensor y el reclutamiento con el mismo sensor. Esto es debido a que las huellas que se están comparando se han obtenido de la misma manera por lo que a la hora de compararlas se obtienen muchos menos errores. En cuanto a las pruebas de interoperabilidad cruzadas, se obtienen unos errores muy parecidos tanto si se hace el reclutamiento con un sensor óptico y el reconocimiento con el capacitivo como viceversa.

Se ha de tener en cuenta que las imágenes obtenidas de los dos sensores son distintas por lo que se obtiene distintos rendimientos para cada sensor. En el óptico la superficie que se obtiene es mayor que en el capacitivo por lo que las muestras tienen mayor número de puntos característicos y de ahí que se cometan menos errores en el óptico.

El análisis de usabilidad proporcionó información interesante según los sensores. Se ha podido observar que los sensores con los que más errores se han cometido fueron con el de huella rodada y con el capacitivo. Se vincula de este modo el análisis de usabilidad al de rendimiento. Comparten el hecho de que el sensor capacitivo causó más errores y tuvo un menor rendimiento. En cuanto al sensor óptico tuvo menos errores y mayor rendimiento que el capacitivo.

Cabe destacar la relación existente entre usabilidad y el rendimiento obtenido de los sensores. Se ha podido observar que el sensor capacitivo no contaba con buena usabilidad debido a la cantidad de errores que se cometían con él. Sin embargo, el sensor óptico 1 no causó tantos errores. Es por ello que el rendimiento del sensor óptico era mucho mayor que el del capacitivo y que la interoperabilidad entre ellos resultó ser muy baja.

6.2. Líneas futuras

Como líneas futuras de investigación se piensa especialmente en seguir mejorando los sistemas de reconocimiento biométrico, tanto en usabilidad como en rendimiento.

Se ha comentado en el apartado 3.1.1.3 que el archivo log registraba los errores que ocurrían pero hay ciertos errores de los que es imposible tener conciencia si no es con una grabación de vídeo. De ahí que si se pudiera grabar el proceso de la captura de las huellas dactilares, se obtendría información de errores que de otra manera no serían tenidos en cuenta.

Se piensa especialmente en realizar experimentos como los realizados pero variando los sensores. Cambiar la tecnología y cambiar la manera en la que los sensores capturan la muestra. De este modo se podrá comparar los resultados de este TFG y tener una visión más global de la situación.

Para obtener unos mejores resultados se podría realizar las pruebas con una BBDD que estuviera formado por más usuarios para aumentar el número de huellas y de este modo obtener resultados estadísticamente más significativos. Además sería recomendable que se obtuvieran muestras de personas de todo tipo, variando lo máximo posible. Por ejemplo la raza, la edad o la ocupación ya que en este TFG la mayoría compartían estas características.

Paralelamente se podrían realizar estos mismos experimentos para los distintos dispositivos según las modalidades biométricas como el iris o el reconocimiento de voz.

Por último, continuando con el estudio de la usabilidad, se podría continuar simplemente analizando el resto de parámetros que no se han analizado como las visitas o los dedos ya que podrían dar información muy interesante.

Bibliografía

[1] La normalización en el campo de la identificación biométrica. http://www.revistadintel.es/Revista/Numeros/Numero1/Normas/Sanchez.pdf
Última consulta: 9 de junio de 2014

[2] Ley Orgánica 15/1999. http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html
Última consulta: 9 de junio de 2014

[3] Search Data Center, definición biometría http://searchdatacenter.techtarget.com/es/definicion/Biometria
Última consulta: 9 de junio de 2014

[4] Sistemas biometría, definición biometría http://sistemasbiometria.blogia.com/temas/definicion-biometria.php
Última consulta: 9 de junio de 2014

[5] Iris http://www.oracleyyo.com/index.php/2013/07/17/expdp_en_vistas
Última consulta: 9 de junio de 2014

[6] Facial 2D http://www.sistemasbiometricos.cl/web/2012/08/27/red-de-justicia-de-pennsylvania-tendra-tecnologia-de-reconocimiento-facial/
Última consulta: 9 de junio de 2014

[7] Facial 3D http://www.madrimasd.org/noticias/nueva-base-datos-perfecciona-sistemas-reconocimiento-facial/40874
Última consulta: 9 de junio de 2014

[8] La firma de puño y letra es un rasgo biométrico http://www.stepover.es/info/la-firma-electronica/biometria.html
Última consulta: 9 de junio de 2014

[9] Tests de ADN http://expertadn.fr/
Última consulta: 9 de junio de 2014

[10] ISO/IEC JTC1/SC37 Biometrics, "SC37 Standing Document 11(SD11), Part 1 Harmonization Document, Mayo 2008.

[11] Sánchez Ávila, Carmen, Aplicaciones de la biometría a la seguridad.

[12] ROC DET CMC EER -- N. Y. Ted Dunstone, Biometric System and Data Analysis - Design, Evaluation and Data Mining, Springer, 2009, p. 276.

[13] Institute of Electrical and Electronics Engineers. IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries. New York, NY: 1990.

[14] Fernández Saavedra, Mª Belén, Biometría y la evaluación de los sistemas biométricos

[15] Sasse, M.Angela, Usability and Trust in Information Systems

[16] Stephen J. Elliott, Eric P. Kukula, A Definitional Framework for the Human-Biometric Sensor Interaction Model

[17] Científicos explican por qué hay tan pocos zurdos en el mundo
http://www.abc.es/20120429/ciencia/abci-zurdos-poco-comunes-201204271336.html
Última consulta: 9 de junio de 2014

Anexo A: Planificación

En este anexo se detalla la planificación que se ha seguido para este trabajo y su equivalencia en horas.

Fase 1: Documentación inicial
I. Asistencia a presentaciones sobre Biometría (10 horas)
II. Estudio de la Biometría (10 horas)
III. Preparación de las herramientas de trabajo (2 horas)

Fase 2: Obtención de la base de datos
I. Explicación y aprendizaje de la aplicación de recogida de huella (3 horas)
II. Recogida de huellas (50 horas)

Fase 3: Desarrollo de las aplicaciones
I. Obtención de tasas de rendimiento y usabilidad (20 horas)
II. Pruebas de las aplicaciones (10 horas)
III. Mejora de las aplicaciones (25 horas)

Fase 4: Pruebas finales
I. Obtención de resultados de comparación de los experimentos (20 horas)
II. Estudio de los resultados (20 horas)

Fase 5: Elaboración de la memoria
I. Redacción de la memoria (80 horas)
II. Corrección (20 horas)

Tabla 17 – Duración del TFG

Fase	Horas
Documentación inicial	22
Obtención de la BBDD	53
Desarrollo de las aplicaciones	55
Pruebas finales	40
Elaboración de la memoria	100
TOTAL	**300**

Anexo B: Presupuesto

En este segundo anexo se van a plasmar los costes que han sido necesarios para el trabajo. Se clasifican en dos grupos principales: Costes de materiales (tabla 18) y costes de personal (tabla 19). El resultado final se obtiene en costes totales (tabla 20).

No han sido incluidos los costes derivados de las licencias del software ya que se dispone de estas licencias.

Costes materiales

El hardware necesario para este trabajo ha sido 2 ordenadores y 4 sensores de huella dactilar.

Tabla 18 - Costes materiales

Concepto	Cantidad (€)
2 ordenadores altas prestaciones	800
8 sensores huella dactilar	800
TOTAL	**1600**

Costes de personal

Para realizar este trabajo ha sido necesario el trabajo de un ingeniero y de un jefe de proyecto.

Tabla 19 - Costes de personal

Puesto	Nº horas	€/hora	Cantidad (€)
Jefe de proyecto	280	50	14000
Ingeniero	20	90	1800
Total	**300**	**-**	**15800**

Costes totales

Tabla 20 - Costes totales

Concepto	Cantidad (€)
Costes materiales	1600
Costes de personal	15800
Subtotal	**17400**
IVA (21%)	3654
Total	**21054**